3/2014

Datenschutz Nachrichten

37. Jahrgang
ISSN 0137-7767
12,00 Euro



Datenschutz im Reiseverkehr

■ Quo vadis Massenüberwachung? ■ Erfassung und Nutzung von Standortdaten ■ Videoüberwachung in Taxen ■ Gläserne Touristen zwischen Big Data und Staatsüberwachung ■ Drohnen und Datenschutz ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Freitag, 10. Oktober 2014, 18:00 Uhr
„Von Shitstorms, Speckrollen und dem Streisandeffekt“ – unterwegs in Sozialen Netzwerken. Vortrag zu sozialen Netzwerken an der THM
Referenten: Christoph Palmert, Jens-Oliver Müller
Technische Hochschule Mittelhessen – Campus Gießen, Gebäude A 20, Hörsaal 1.36 (1. OG) (vormals Gebäude I), Wiesenstraße
http://www.thm.de/datenschutz/veranstaltungen

Samstag, 18. Oktober 2014, 16:00 Uhr
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle.
dvd@datenschutzverein.de

Sonntag, 19. Oktober 2014, 10:00 Uhr
Mitgliederversammlung
Bonn. Gesonderte Einladung folgt.
Anmeldung in der Geschäftsstelle erbeten.

Samstag, 01. November 2014
Redaktionsschluss DANA 4/2014
Thema: Big Data
Verantwortlich: Jaqueline Rüdiger

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
37. Jahrgang, Heft 3

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Frans Jozef Valenta
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserinnen und Leser,

ursprünglich sollte sich dieses Heft mit „Datenschutz im Flugverkehr“ beschäftigen. Für diese Thematik war unter anderem ein Interview zu Gepäckkontrollen mit der Bundespolizei am Flughafen Köln-Bonn vorgesehen. Ein besonders wichtiger Aspekt war dabei die Art und Weise, wie die Wahrung der Privatsphäre bei den öffentlichen Kontrollen gewährleistet wird. „Mit Blick auf die Bedeutung des Sachverhalts“ wurden die Fragen an die Bundeszentrale in Potsdam weitergeleitet. Die Antworten lagen eine Woche vor der Drucklegung der Datenschutz Nachrichten noch nicht vor. Sie werden möglicherweise erst im nächsten Heft veröffentlicht werden können.

Wegen einiger der inzwischen hinzugekommenen Artikel war eine Erweiterung auf „Datenschutz im Reiseverkehr“ angebracht.

Ein großes Ärgernis für den Datenschutz im Flugverkehr sind die Passenger Name Records (PNR). Jan Philipp Albrecht, MdEP, betrachtet den aktuellen Stand der Diskussion in der EU. Im Reiseverkehr werden immer intensiver Standortdaten gesammelt. Der Artikel von Achim Klabunde beleuchtet die Erfassung innerhalb des europäischen Rechtsrahmens. Die Videoüberwachung in Taxen, einem oft benutzten Transportmittel im Zusammenhang mit Bahnhöfen und Flughäfen, ist das Thema von Tobias Jaquemain. In einem Interview beantwortet Thilo Weichert Fragen zum gläsernen Touristen. Mit Videokameras ausgestattete Miniatur-Drohnen entwickeln sich immer mehr zu einer erschwinglichen und beliebten Freizeitbeschäftigung, die allerdings eine Reihe von Fragen zum Datenschutz aufwirft. Stephan Möhrle gibt hierzu einen Überblick.

Frans Jozef Valenta

Autorinnen und Autoren dieser Ausgabe:

Jan Philipp Albrecht
Innen- und justizpolitischer Sprecher der Grünen im Europäischen Parlament sowie Berichterstatter des Europäischen Parlaments für die neue EU-Datenschutzverordnung.
jan.albrecht@europarl.europa.eu

Tobias Jacquemain
Studium der Volkswirtschaftslehre und des Europarechts (LL.M.) in Köln und Saarbrücken. Derzeit wissenschaftlicher Mitarbeiter von Univ.-Prof. Dr. Karl Lauterbacht, MdB.
jacquemain@web.de

Achim Klabunde
Leiter des Sektors IT-Politik beim Europäischen Datenschutzbeauftragten.
achim.klabunde@edps.europa.eu
Der Artikel gibt ausschließlich die persönliche Meinung des Autors wieder.

Stephan Möhrle
Mitglied im Sprecherkreis des DFG-VK-Landesverbands Baden-Württemberg und Jura-Student an der Johannes-Kepler-Universität Linz.
moehrle@dfg-vk.de

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel.
weichert@datenschutzzentrum.de

Jan Philipp Albrecht

Fluggastdaten
Quo vadis Massenüberwachung?



Bild: ClipDealer.de

Nach dem wegweisenden Urteil des Europäischen Gerichtshofs über die Unvereinbarkeit der EU-Richtlinie zur Vorratsdatenspeicherung mit der Grundrechtecharta der Europäischen Union stellt sich die Frage, inwieweit dieses Urteil nicht bloß die anlasslose Speicherung von Telekommunikationsdaten auf Vorrat betrifft, sondern auch die anderen Maßnahmen anlassloser Verarbeitung personenbezogener Daten auf Vorrat, wie etwa die Erhebung, Speicherung und Analyse von so genannten Passenger Name Records (PNR), einfacher: Fluggastdaten.[1] Bereits vor der Verabschiedung der Vorratsdatenspeicherung im Telekommunikationsbereich war nach dem 11. September 2001 in den Vereinigten Staaten durch das damals neu gegründete US-Heimatschutzministerium die Verpflichtung an alle Fluggesellschaften ergangen, die PNR-Daten der einreisenden Fluggäste anlasslos und umfangreich zum Zwecke der Terrorismusabwehr zur Verfügung zu stellen. Wegen der langwierigen und kostspieligen Umstellung der Systeme sah man dabei von der aktiven Übermittlung der Daten durch die Fluggesellschaften gleich ab und verpflichtete sie, einen Zugang zu ihren Daten auf den Buchungsgesellschaftssystem zu gewähren. Diese Jahrzehnte alten Datenverarbeitungssysteme (die auf Grund ihrer Entstehung noch immer jeglichen angemessenen Datenschutzes entbehren) verarbeiten die Flugpassagierdaten aller weltweiten Flugbuchungen; drei der vier großen Serversysteme sitzen in den USA, eine in Europa.

Unter strengster Geheimhaltung werden nun seit 2003 in einem Abwehrzentrum des US-Heimatschutzministeriums im Bundesstaat Virginia die Informationen aller rund 30 Millionen Fluggäste, die jährlich in die USA einreisen oder diese verlassen, analysiert und mit anderen Ermittlungsinformationen verknüpft. Dazu zählen weitreichende Buchungsrahmendaten der Reiseagenturen und Luftverkehrsgesellschaften, etwa Kreditkartendaten, Handynummer, die IP-Adresse des Buchungsvorgangs und Hotel- oder Mietwagenreservierungen. All diese Informationen fließen in detaillierte Gefahrenanalysen ein, die mithilfe geheimer Algorithmen (wiederum auf Grundlage der auf Jahrzehnte gespeicherten PNR-Daten) erstellt und anschließend ausgewertet

werden. Aufgrund der weitreichenden Befugnisse des US-Heimatschutzministeriums bleibt für die Reisenden (und die Datenschutzbehörden) dabei völlig unklar, welche Datensätze miteinander verknüpft und welche weiteren Überwachungsmaßnahmen daraufhin angeordnet werden. Zahlreiche Beispiele belegen, dass bereits ungewöhnliche Namen oder auffällige Menüwünsche im Flugzeug verdächtig wirken können – im schlimmsten Fall führen die Indizien gar zum dauerhaften Einreiseverbot. Vor allem aber haben die Betroffenen keinen Einfluss auf mögliche Fehleinschätzungen der Ermittler, da es ihnen nicht gestattet ist, die erhobenen Daten einzusehen, geschweige denn korrigieren oder löschen zu lassen. Insbesondere europäische Flugreisende sind dieser Überwachung ausgeliefert – für die Verarbeitung der persönlichen Daten von EU-Bürgerinnen und Bürgern gab es zu Beginn nicht einmal eine Rechtsgrundlage im europäischen Recht, so dass die Fluggesellschaften regelmäßig gegen den Datenschutz verstießen, wenn sie den US-Behörden die Daten zur Verfügung stellten. Erst auf Druck des Europäischen Parlaments begannen Verhandlungen zwischen den USA und der EU. Das Parlament hatte in mehreren Resolutionen das Vorgehen der Vereinigten Staaten scharf verurteilt und infolgedessen auch erfolgreich vor dem Europäischen Gerichtshof gegen die zunächst vom Ministerrat verabschiedeten Abkommen geklagt. Nach dem Inkrafttreten des Vertrags von Lissabon, der dem Europäischen Parlament erheblich mehr Mitbestimmung einräumt, musste ein Abkommen über die Weitergabe der PNR-Daten an die US-Behörden neu verhandelt werden. Mehrere Entwürfe wurden von den Abgeordneten zurückgewiesen; erst nach intensiven Neuverhandlungen mit den Vereinigten Staaten fand sich eine Mehrheit aus den Fraktionen EVP, S&D und ALDE für ein Abkommen, dass den Datentransfer heute regelt. Washington hatte zuletzt sogar mit dem dauerhaften Entzug der Landeerlaubnis für europäische Fluglinien gedroht.

Die im Abkommen EU-USA vorgesehene Speicherdauer von bis zu 15 Jahren deutet bereits auf den weitgehenden Bruch mit grundlegenden Verhältnismäßigkeitsgrundsätzen in der EU hin. Angesichts des Urteils aus dem April 2014 ist zu erwarten, dass eine Klage vor dem Europäischen Gerichtshofs gegen dieses Abkommen ebenso erfolgreich beschieden würde, wie die gegen die Richtlinie zur Vorratsdatenspeicherung. Unglücklicherweise ist der Klageweg für einzelne Betroffene bei diesem Abkommen noch steiniger als gegenüber der Vorratsdatenspeicherungsrichtlinie. Denn während bei der EU-Richtlinie EG/24/2006 noch Umsetzungsgesetze durch die Mitgliedstaaten zu verabschieden waren, gegen die sich die Kläger aus Österreich und Irland gewehrt hatten, ist der Rechtsweg gegen ein reines EU-Abkommen vor nationalen Gerichten ausgeschlossen. Die Individualklage aus Grundrechtsbetroffenheit allerdings hatte der Europäische Gerichtshof – zumindest bislang – immer sehr restriktiv bis ablehnend beschieden. Lediglich die Klage gegenüber der Fluggesellschaft, die in einigen EU-Ländern anhängig ist, könnte per Vorlageverfahren vor dem Luxemburger EU-Gericht landen und dann eine Beendigung des PNR-Abkommens bewirken, wenn dieses feststellt, dass die Fluggesellschaften zumindest auf dieser Rechtsgrundlage keinen Datentransfer hätten durchführen oder zulassen dürfen. Noch scheint es hierzu aber zu wenige und schlecht ausgestattete Klägerinnen und Kläger zu geben und zu wenige nationale Richter, die ihrer Verantwortung im Rechtssystem der EU umfassend nachkommen und den Fall dem EuGH vorlegen.

Für die Befürworter einer Ausweitung von Überwachungsmaßnahmen in Europa war die Verabschiedung des Abkommens mit den USA (und nahezu parallel dazu mit Australien und Kanada – ein darauf folgender Wunsch Russlands und Katars nach ähnlichen Abkommen wurde seitens der EU-Kommission zurückgewiesen) eine Gelegenheit, die Auswertung der PNR-Daten auch in der EU salonfähig zu machen. Hatte die schwedische liberale EU-Kommissarin Cecilia Malmström noch vor wenigen Jahren als EU-Parlamentarierin gegen die massenhafte Auswertung von Fluggastdaten durch US-Behörden argumentiert, legte sie im Februar 2012 dann auf Druck der Innenminister der EU-Staaten selbst einen Vorschlag für ein europäisches Fluggastdaten-Analyseprogramm vor – das dem US-amerikanischen Überwachungsapparat in nichts nachsteht. Zugleich verharmloste Malmström die Dimension des Vorhabens und bewarb es, ironischerweise, als handle es sich um ein Datenschutzgesetz. Die Absicht der Kommissarin war in der Folge klar erkennbar: Sie wollte mit allen Mitteln den Eindruck vermeiden, die Vorratsdatenspeicherung diene der Rasterfahndung oder gar dem sogenannten Profiling, wo unterschiedliche Informationen zu „Gefährderprofilen“ zusammengeführt werden. Doch genau das wäre der Fall. Auch im EU-System sollen Passagiername, Reisezeiten und -routen, Kontaktangaben, das beauftragte Reisebüro, die Zahlungsart, ja sogar die Sitznummer im Flieger sowie genaue Angaben über das aufgegebene Gepäck gespeichert werden. All diese Informationen sollen durch mitgliedstaatliche Stellen automatisch analysiert werden. Erklärtes Ziel des vorgelegten Richtlinienvorschlags ist es, Terroristen und Drogenschmuggler aufzuspüren.

Einzelne Staaten wie Großbritannien und Spanien forderten im Ministerrat dann sogar noch einen Schritt weiter zu gehen, als es die EU-Kommission vorsah. Sie beantragten, PNR-Daten fortan auch bei innereuropäischen Flügen anlasslos zu sammeln. Mitte April 2012 hat sich dann auch eine Mehrheit auf dem EU-Innenministertreffen in Luxemburg für diesen Vorschlag ausgesprochen. Nachdem der Kommissionsvorschlag für die Richtlinie im Frühjahr 2012 auch den Abgeordneten des Europäischen Parlaments zugeleitet wurde, entfachte er dort in Folge der Debatten über die Datenabkommen der vergangenen zwei Jahre (inklusive der Zurückweisung der ersten Abkommen zu SWIFT-Daten und PNR-Daten an die USA) eine harte Auseinandersetzung zwischen dem britischen konservativen Berichterstatter und der damaligen links-liberal-grünen Mehrheit im zuständigen Innen- und Justizausschuss. Viele sahen die Fluggastdatenüberwachung im Stile der USA bereits in den Jahren 2012 und 2013 im deutlichen Widerspruch zur Datenschutzrechtsprechung in der Europäischen Union und damit als Bedrohung zentraler rechtsstaatlicher Prinzipien. Trotz zahlreicher Versuche der Briten

(die mit ihrem Secure Flight Program bereits ein ähnliches System installiert haben, wie die US-Amerikaner) und der Generaldirektion Innen der EU-Kommission, die Parlamentarier von der Wirksamkeit und Notwendigkeit eines EU-weiten Fluggastdatensystems zu überzeugen, gelang dies nicht. Der Innen- und Justizausschuss sprach sich mit der Mehrheit der Fraktionen S&D, Liberale, Linke und Grüne für die Zurückweisung der geplanten Richtlinie aus Ganzes aus. Die PNR-Debatte hat sich inzwischen zu einer knallharten politischen Auseinandersetzung zwischen Kommission und Ministerratsmehrheit einerseits und dem Europäischen Parlament andererseits ausgewachsen. Auf Druck der konservativ geführten Regierungen wies sodann das Plenum der Straßburger Abgeordnetenkammer den Beschluss des Innen- und Justizausschuss wiederum zurück; seither gibt es keine neue Position im Europäischen Parlament.

Aber nicht nur Parlamentarier kritisieren die europaweite Überwachung aller Flugreisenden. Auch Beamten in der EU-Kommission und im juristischen Dienst des Rates dämmerte bereits, dass die geplante Richtlinie nicht mit den Einschätzungen der höchsten Gerichte in Straßburg, Luxemburg und Karlsruhe in Einklang zu bringen sein dürfte. Bislang bleiben die Befürworter den vom Europäischen Gerichtshof eingeforderten Nachweis schuldig, dass jede Überwachungsmaßnahme „notwendig und verhältnismäßig in einer demokratischen Gesellschaft“ sein soll. Selbst in als streng geheim eingestuften Berichten werden als Beleg für die notwendige Einführung der Fluggastüberwachung lediglich Einzelfälle angeführt – ohne jedoch die Umstände der jeweiligen Ermittlungen und die Rolle der Fluggastdaten genauer darzulegen. Noch ist die Entscheidung über die Auswertung der europäischen Fluggastdaten nicht gefallen. Zugleich geht es längst nicht mehr allein um die Überwachung des Luftverkehrs: Schon fordert die italienische Regierung eine Ausweitung der Datenerfassung auf sämtliche europäische Fährverbindungen. Und es wird nicht lange dauern, bis auch die Forderung der Überwachung des gesamten Zugverkehrs in Europa wieder von einer Regierung oder der Kommission aufgegriffen wird. Kurzum: Inzwischen droht die vollständige Erfassung und Analyse von Informationen über die Bewegungen der rund 500 Millionen EU-Bürgerinnen und Bürger – in der Luft, zu Wasser und auf dem Lande. Setzen sich die Europäische Kommission und der Rat durch, hätten sie die Überwachungspraktiken der USA nicht nur erfolgreich kopiert, sondern drohten diese in ihrem Umfang bei weitem zu übertreffen. Umso mehr ist zu hoffen, dass das Europäische Parlament den Anfängen dieser Praxis schnell und entschieden einen Riegel vorschiebt.

1 Ausführlich dazu die von der Fraktion der Grünen/EFA im Europäischen Parlament in Auftrag gegebene Studie „Data Retention after the Judgement of the Court of Justice of the European Union“ von Prof. Dr. Franziska Boehm und Prof. Dr. Mark D. Cole: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf (abgerufen am 08.08.2014)

Achim Klabunde

Datenschutz bei der Erfassung und Nutzung von Standortdaten

Europäischer Rechtsrahmen zur Verarbeitung von Standortdaten

Im Rechtsrahmen der Europäischen Union für die elektronische Kommunikation, der im Rahmen der Liberalisierung der Telekommunikationsmärkte in den 90er Jahren des letzten Jahrhunderts entwickelt und in den Jahren 2002 und 2009 reformiert wurde, bemühte sich der Gesetzgeber, auch den Datenschutzanforderungen der neuen digitalisierten Kommunikationsdienste Rechnung zu tragen. Dabei ging es auch darum, den Datenschutz gegenüber den Interessen der privaten Netzbetreiber zu gewährleisten. Bereits die Richtlinie 97/66/EG[1] fasste dazu nicht nur das Grundprinzip des Fernmeldegeheimnisses in eine Vorschrift, die in nationales Recht umgesetzt werden muss, sondern berücksichtigte auch die durch die digitale Technik geschaffenen neuen Möglichkeiten der Erfassung von Daten über Telekommunikationsvorgänge. Sie regelte den Umgang mit Anrufer-Identifikation, Rechnungen mit Einzelgebührennachweis, die für jedes Gespräch Zeit, Dauer und Nummern der Teilnehmer erfassen, die Regeln zur Erfassung und Verarbeitung von heute als Metadaten bekannten Informationen über die Kommunikationen der Nutzer (Verkehrs- und Abrechnungsdaten), sowie weitere Regeln etwa zur Wahlfreiheit der Nutzer über ihre Eintragung in Telefonverzeichnisse und zu unerwünschten Anrufen. Bei der ersten Überprüfung des Rechtsrahmens im Jahre 2002 wurde die Richtlinie durch eine Neufassung[2] ersetzt und ihr Regelungsumfang erweitert. Die Regelungen der vorherigen Richtlinie wurden im Wesentlichen vollständig übernommen und teilweise erweitert, z. B. indem die Regelung für unerwünschte Nachrichten nicht mehr nur für Telefonanrufe, sondern auch für E-Mail



Bild: ClipDealer.de

und andere Dienste gilt. Die Regelungen zum Fernmeldegeheimnis wurden durch einen Absatz zum Schutz der Integrität der Teilnehmergeräte ergänzt, der vor allem durch seine Anwendung auf Cookies bekannt wurde. Neu hinzugefügt wurde ein Artikel über die Verarbeitung von Standortdaten[3].

Aus heutiger Sicht zeigt die Fassung dieses Artikels von 2002 einen erstaunlichen Weitblick des Gesetzgebers zur Bedeutung von Standortdaten und der Risiken ihrer unbegrenzten Nutzung. Diese Einsicht zeigt sich in sehr klaren Regeln über die Nutzung von Standortdaten: Soweit sie nicht für Übertragungs- oder Abrechnungszwecke verwendet werden, können sie nur für Zusatzdienste und nur anonymisiert oder mit Einwilligung des Nutzers oder Teilnehmers verwendet werden. Vor Erteilung der Einwilligung muss der Nutzer über die Art der Daten, die Verarbeitung, deren Dauer und eventuelle Weitergabe an Dritte informiert werden. Die Einwilligung kann jederzeit widerrufen werden, auch zeitweise oder für einzelne Kommunikationsakte, ohne dass dem Betroffenen Kosten entstehen. Diese Regelungen sind deutlich strenger als die allgemeinen Bedingungen für die Verarbeitung personenbezogener Daten unter der EU-Datenschutzrichtlinie[4]. Insbesondere sind berechtigte Interessen der verantwortlichen Stelle nicht als ausreichender Rechtsgrund für die Verarbeitung zugelassen. Die Richtlinie betont auch ausdrücklich die Prinzipien der Zweckbindung, der Datensparsamkeit und der Zeitbeschränkung. Die Regelungen für Standortdaten sind auch strenger als die in der selben Richtlinie enthaltenen Bestimmungen für Verkehrs- und Abrechnungsdaten, bei denen eine Nutzung für die Vermarktung von Diensten ausdrücklich zugelassen ist. Im Rahmen der Überprüfung des Rechtsrahmens für elektronische Kommunikation 2009 wurden die Bestimmungen zu Verkehrs-, Abrechnungs- und Standortdaten unverändert gelassen.

Während der EU-Gesetzgeber die besonderen Risiken der Verarbeitung von genauen Standortdaten klar erkannt hat und hier den privaten Dienstleistern strenge Regeln auferlegte, hat er der Nutzung durch Sicherheits- und Strafverfolgungsbehörden größeren Spielraum gelassen. Nicht nur gibt die Richtlinie 2002/58/EG selbst den Mitgliedsstaaten das Recht, durch nationale Gesetze u. a. für Zwecke der Sicherheit und Strafverfolgung Ausnahmen von den Schutzvorschriften zu bestimmen, ausdrücklich auch für eine längere Aufbewahrung der Daten, sondern 2006 wurde sogar eine Verpflichtung zu einer solchen längerfristigen Speicherung mit der Vorratsdatenspeicherungsrichtlinie[5] geschaffen. Diese Richtlinie sah eine Verpflichtung für längerfristige Speicherung von Metadaten, inklusive der Standortdaten, zu Beginn jeder Mobilkommunikation vor. Wie der Gerichtshof der Europäischen Union inzwischen feststellte, wurden diese Bestimmungen allerdings ohne die notwendige Prüfung der Notwendigkeit und Verhältnismäßigkeit eingeführt. Mit dem EUGH-Urteil[6] vom 8. April 2014 wurde die Vorratsdatenspeicherungs-Richtlinie aufgehoben. Der Effekt auf nationale Gesetze ist aber nicht einheitlich. Während in einigen Mitgliedsstaaten Verfassungsgerichte die nationalen Gesetze aufhoben, hat das Parlament des Vereinigten Königreichs im Juli 2014 im Eilverfahren ein neues weitreichendes Gesetz[7] verabschiedet. Welche rechtliche Wirkung das EUGH-Urteil auf dieses und andere bestehende nationale Vorratsdatenspeicherungsgesetze haben wird, ist noch nicht klar. Ob die Ausnahmeregelung der Richtlinie 2002/58/EG für eine Vorratsdatenspeicherung unter bestimmten Voraussetzungen ausreicht, muss unter Berücksichtigung der im EUGH-Urteil ausgearbeiteten Grundsätze über die Interpretation der Charta der Grundrechte der Europäischen Union geprüft werden.

Neue technische Möglichkeiten zur Erfassung von Standortdaten

Seit der Einführung des Standortdatenartikels hat sich die Technologie massiv weiterentwickelt. Während im Jahre 2002 die Nutzung von Standortdaten aus Mobilfunknetzen in der Tat noch die Spitze der angewandten technischen Entwicklung darstellte, ortsbasierte Dienste („location based services“) für viele Netzbetreiber das Stadium der Planung und der Marketingversprechen

noch nicht verlassen hatten, und auch die Vorstellungen über den wirtschaftlichen Wert solcher Dienste noch sehr vage waren, hat sich auf dem Gebiet der Ortungsdaten in den letzten 12 Jahren eine ungeheure Entwicklung vollzogen. Standortdaten werden heute auf so viele verschiedene Weisen und von so vielen verschiedenen Akteuren gesammelt, dass die Nutzung der Zellkoordinaten von Mobiltelefonen für Mehrwertdienste schon fast als eine der harmloseren Varianten erscheinen könnte. Allerdings hat sich auch auf diesem Gebiet viel geändert: Die Anzahl der mobilen Telefone hat sich vervielfacht; viele Geräte verfügen über drei oder mehr unabhängige Möglichkeiten zur Standortermittlung; und auch standortbezogene Dienste haben sich massiv entwickelt. In seinem Jahresbericht[8] 2013 hat der Europäische Datenschutzbeauftragte Beobachtungen über die technische Entwicklung von Datenerfassungs- und Verarbeitungs-Systemen veröffentlicht, die hier wiedergegeben sind.

Aber insbesondere außerhalb des Kommunikationssektors nimmt die Erfassung von Ortungsdaten und deren Nutzung für verschiedene gewerbliche Zwecke weiter zu. Während viele kleinere und größere Anbieter standortbasierter Dienste in begrenztem Umfang Standortdaten ihrer Nutzer erfassen oder verarbeiten, gibt es einige wenige Akteure, die solche Daten permanent und in großem Umfang erfassen, insbesondere die Hersteller der Smartphones und der zentralen Anwendungen auf diesen Geräten. Durch die wachsende Konzentration im Markt für Mobilgeräte und Kommunikationsdienste wird die Rolle dieser wenigen weltweit führenden Akteure weiter gestärkt.

Außer der netzbezogenen Ortserfassung und satellitengestützten Ortsbestimmung (GPS) werden auch andere Ortungsmechanismen verwendet, beispielsweise beim Bluetooth- und WiFi-Tracking und beim Tracking von Mobiltelefonen auf kurzen Entfernungen, die über die abgegebenen Funksignale oder bei einer Interaktion mit diesen Geräten erfolgt. Hinzu kommt, dass auch viele andere Geräte mittlerweile mit Kommunikations- und Tracking-Funktionen ausgestattet sind, beispielsweise biometrische Sensoren für sportliche Aktivitäten, Satellitennavigationssysteme, automatische Mautzahlungssysteme und elektronische Fahrkarten für den öffentlichen Nahverkehr (Internet der Dinge).

Verkehr

Der Einbau von Kommunikations-, Ortungs- und Datenverarbeitungssystemen in Kraftfahrzeugen wird weiter zunehmen, nicht zuletzt im Zuge der geplanten flächendeckenden Verbreitung eines eCall-Systems, das nach Vorschlag der Europäischen Kommission und des Parlaments ab 2015 in allen neuen Personenkraftwagen in Europa eingebaut werden soll. Die Verbreitung solcher Plattformen wird das Interesse wecken, sie nicht nur für Notrufdienste, sondern auch für andere Dienste zu nutzen. Vorschläge wie der, die Kraftfahrzeugversicherungsbeiträge anhand der Fahrleistung zu bemessen und dabei auch gezielt die benutzten Strecken sowie das Verhalten des Fahrers (z. B. häufiges Beschleunigen und Bremsen) zu berücksichtigen, sind nur ein Beispiel für die kreativen Ideen, die es für die Verwendung von Mobilitätsdaten gibt.

Auch andere Erfassungssysteme im Straßenverkehr werden zur Sammlung von Ortsdaten genutzt. Immer häufiger werden Forderungen laut, Kennzeichenerkennungsdaten aus bestehenden Mautsystemen auch für Strafverfolgungszwecke zu nutzen, ebenso wie Daten aus Geschwindigkeitskontrollsystemen, die an Autobahnauf- und -abfahrten die Kennzeichen von Fahrzeugen erfassen, um deren Durchschnittsgeschwindigkeit im betreffenden Streckenabschnitt zu ermitteln.

Im öffentlichen Personenverkehr werden zunehmend elektronische Tickets eingesetzt, für die Standort und Uhrzeit bei jeder Benutzung erfasst werden können. Der Nahverkehr wird zunehmend auch mit Stadtauto- oder Leihfahrrad-Systemen ergänzt, die mit denselben oder ähnlichen Karten genutzt werden können und das Netz der Ortserfassung weiter verdichten.

Das Internet der Dinge

Im „Internet der Dinge“ sollen Alltagsgegenstände wie Telefone, Autos, Haushaltsgeräte, Kleidungsstücke und andere Geräte Internetprotokolle nutzen, um drahtlos miteinander Daten austauschen und untereinander kommunizieren zu können. Es ist ein wesentlicher Bestandteil für Konzepte wie die Intelligente Stadt (smart city), die ein besseres Management der Städte durch massenhafte Sammlung und Verarbeitung von Daten und die Steuerung von Infrastrukturkomponenten erreichen soll.

Einheitliche Normen und Systeme, die herstellerübergreifend Kommunikation zwischen Geräten ermöglichen würden, existieren noch nicht. Stattdessen haben viele Anbieter Lösungen für bestimmte Anwendungen entwickelt, um diese mithilfe der vorhandenen Infrastruktur zu vernetzen. Aus diesem pragmatischen Ansatz heraus ist eine breite Palette von Geräten entstanden, die Informationen über Personen erfassen und an verschiedene Webdienste übermitteln, z. B. bei Sportmessgeräten. Die Sensoren kommunizieren nur selten auf gleicher Ebene miteinander oder mit den Geräten der Nutzer, sondern übermitteln stattdessen Daten an zentrale Cloud-Computing-Dienste. Dadurch sammeln die Anbieter riesige Mengen an personenbezogenen Daten, die auch für andere Zwecke ausgewertet und genutzt werden könnten.

Datenminimierung und Zweckbindung könnten die entstehenden Datenschutzrisiken begrenzen, aber es gibt nur wenige oder gar keine Anreize für die Entwickler der Software für das Internet der Dinge, in Datenschutz- und Sicherheitsmaßnahmen zu investieren. Experten befürchten, dass derzeit die nächste Generation einer wichtigen, aber unsicheren Infrastruktur entsteht, weil keine Regeln für eingebettete Geräte vorgegeben werden.

Gesichtserkennung und Überwachungssysteme

Durch Fortschritte in der Gesichtserkennungstechnologie und die stetig wachsende Menge an visuellen Informationen, die ins Internet gestellt werden, ist es einfacher geworden, Fotos mit weiteren personenbezogenen Daten zu verbinden, inklusive eindeutiger Identifikationsdaten. Mit der gleichzeitigen Verbreitung hochauflösender Videoüberwachungsanlagen wird es vermehrt möglich, automatisch die im

Bild erfassten Personen zu identifizieren. Festinstallierte Überwachungsanlagen werden anlassbezogen durch unbemannte fliegende Systeme (Drohnen) ergänzt.

Weiterentwickelte Systeme für Grenzkontrollen und Zugangskontrollsysteme erfassen sehr genau, wenn auch nur punktuell, Daten über die Aufenthaltsorte von Personen.

Aktuellen Medienberichten zufolge werden für die zunehmenden staatlichen Überwachungsmaßnahmen auch Standortdaten aus privaten Diensten verwendet. Dies kann durch offizielle Anfrage, durch technische Maßnahme wie stille SMS, aber auch durch Manipulation von Endgeräten geschehen, beispielsweise durch heimliche Installation einer Spähsoftware auf dem Gerät eines bestimmten Nutzers. Mit mobilen Anwendungen wird der Aufenthaltsort von Mobilgerätenutzern festgestellt.

Aussagekraft und Identifizierbarkeit von Standortdaten

Ironischerweise hat gerade die Vorratsdatenspeicherung dazu beigetragen, die Feinmaschigkeit der Ortserfassung sichtbar zu machen. Im Jahr 2011 hatte der deutsche Politiker Malte Spitz die Herausgabe der über ihn gesammelten Vorratsdaten vor Gericht erstritten und zusammen mit der Wochenzeitung ZEIT eine Visualisierung[9] der Daten erarbeitet, die deutlich zeigt, wie genau bereits die Standortdaten der Telekommunikationsbetreiber über das Leben eines Menschen Auskunft geben. Im Jahr 2014 haben dänische und schweizerische Politiker ähnliche Experimente[10] mit ihren jeweiligen Vorratsdaten durchgeführt.

Standortdaten gelten im Rahmen von Big-Data-Anwendungen als eine der vielversprechendsten Quellen für Auswertungen zu Themen mit geographischem Bezug, z.B. Verkehrs- und Stadtplanung, aber auch für medizinische und Umwelt-Themen. Im Besonderen in der dritten Welt arbeiten auch UN-Organisationen mit Kommunikationsanbietern zusammen, um solche Anwendungen zu entwickeln. Ob Projekte wie Data for Development (D4D)[11] oder Global Pulse[12] wirklich zu entscheidenden Fortschritten bei der Verbesserung der Lebensbedingungen führen werden, oder ob sie nur die Akzeptanz von Big Data erhöhen sollen, muss sich noch zeigen.

Bei der Erfassung einer hinreichend genauen Kette von Standortdaten für eine Person ist die Anonymisierung einer solchen Datenreihe praktisch unmöglich. Selbst wenn sämtliche identifizierenden Attribute wie Namen, Telefonnummern und Gerätekennungen entfernt werden und nur die Orts- und Zeitangaben als Reihe erhalten bleiben, sind diese Reihen so unterschiedlich, dass sie selbst bereits zur Identifizierung dienen können. Dies wurde von einer Untersuchung[13] bestätigt, die die Bewegungsdaten von 1,5 Millionen Menschen aus fünfzehn Monaten untersuchte. Dabei stellte sich heraus, dass bereits vier Datenpunkte ausreichten, um ein Individuum zu identifizieren, selbst wenn die Daten nur stündlich erfasst wurden und die Ortsgenauigkeit den Basisstationen eines Mobilfunknetzes entsprach. Diese Genauigkeit liegt weit unter dem, was heute bereits mit Smartphones erfasst wird.

Datenschutzreform

Der bestehende Rechtsrahmen auf EU-Ebene trägt nur im Rahmen des Telekommunikationsrechts dem besonderen Risiko der Sammlung und Verarbeitung von Standortdaten Rechnung. Im Angesicht der technischen Entwicklung unterliegen daher die wachsenden Sammlungen außerhalb des Bereichs der elektronischen Kommunikation nur dem allgemeinen Datenschutzrecht, das keine besondere Schutzbestimmungen für Standortdaten kennt. Die laufende EU-Datenschutzreform wird daran wenig ändern. Im Gegenteil, die Kommission schreckte eindeutig davor zurück, den Wirtschaftsinteressen an der Nutzung von Ortungsdaten ähnlich wie 2002 enge Grenzen zu ziehen. Im ihrem Entwurf[14] für die neue Datenschutzgrundverordnung veröffentlichte sie den Erwägungsgrund 24, der eine eigenartige Logik benutzt (Hervorhebung vom Autor):

„Bei der Inanspruchnahme von Online-Diensten werden dem Nutzer unter Umständen Online-Kennungen wie IP-Adressen oder Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, zugeordnet. Dies kann Spuren hinterlassen, die zusammen mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der betroffenen Personen zu erstellen und sie zu identifizieren. ***Hieraus folgt, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente als solche nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten sind.****“*

In seiner Stellungnahme[15] zum Verordnungsentwurf der Kommission hat der Europäische Datenschutzbeauftragte seine Zweifel an dieser Argumentation dargestellt und begründet, dass eine der von der Kommission aufgeführten Kennzeichnungen als personenbezogenes Datum behandelt werden muss, wenn sie „mit einer natürlichen Person verknüpft wird, die von dem für die Verarbeitung Verantwortlichen oder jeder anderen Person identifiziert werden kann“. Das gilt natürlich in gleicher Weise für Standortdaten, egal welchen Ursprungs sie sind.

In seinem in erster Lesung verabschiedeten Bericht[16] zum Verordnungsentwurf hat das Europäische Parlament hier etwas mehr Klarheit geschaffen:

(24) ***Diese Verordnung sollte auf eine Verarbeitung angewandt*** *werden, die Kennungen umfasst, die Geräte, Software-Anwendungen und* ***-Tools*** *oder Protokolle liefern,* ***wie etwa IP-Adressen, Cookie-Kennungen und Funkfrequenzkennzeichnungen, es sei denn, diese Kennungen beziehen sich nicht auf eine bestimmte oder bestimmbare natürliche Person.***

Zum Glück hat die Kommission in den materiell-rechtlichen Bestimmungen größere Sorgfalt angewandt und Standortdaten durchaus ausdrücklich in den Rahmen der personenbezogenen Daten einbezogen. Die Bestimmungen der vorgeschlagenen Verordnung erwähnen personenbezogene Standortdaten an verschiedenen Stellen, z.B. in der Begriffsbestimmung und beim Profiling. Insgesamt wird damit klar hervorgehoben, dass Standortdaten als personenbezogene Daten nicht vernachlässigt werden dürfen. Allerdings werden keine besonderen Regelungen

für Standortdaten vorgeschlagen, sondern nur die Anwendung der allgemeinen Datenschutzregeln sichergestellt. Es wird damit das allgemeine Schutzniveau der personenbezogenen Daten erreicht; es werden nicht die strikteren Prinzipien aus dem Bereich der elektronischen Kommunikation angewandt. Hier besteht die Gefahr eines erheblichen Ungleichgewichts zwischen Risiko und Schutz. Aus Sicht des Datenschutzes wäre aber das Gegenteil richtig, d.h. eine Anhebung für alle Verarbeiter von Standortdaten auf das Niveau der TK-DS-Richtlinie, also eine Verarbeitung nur bei ausdrücklicher Zustimmung der Betroffenen nach umfassender und genauer Information. Es erscheint fraglich, ob dies im Prozess der DS-Reform erreicht werden kann. Nicht nur ist der Bericht des EP hierauf nicht eingegangen, auch sonst ist methodisch die Behandlung von solchen speziellen Fragen im ohnehin umfangreichen Datenschutz-Instrument möglicherweise nicht optimal.

Ein anderer Ansatz, ein angemessenes Niveau für den Schutz von Standortdaten zu erreichen, könnte daher eventuell eine Ausweitung des Anwendungsbereiches des Standortdaten-Artikels der Kommunikationsdatenschutz-Richtlinie 2002/58/EG auf alle verantwortlichen Stellen sein, die Standortdaten erfassen und verarbeiten, auch wenn sie keine TK-Unternehmen sind. Auch einige andere Bestimmungen dieser Richtlinie, wie etwa das Verbot des Eingriffs in Benutzerterminals oder die Regeln gegen Spam gelten bereits für Akteure außerhalb des Bereichs der Telekommunikation. Die Kommission hat eine Reform dieser Richtlinie angekündigt und dazu im Frühjahr eine Studie[17] beauftragt, die auch insbesondere den Umfang der Anwendung der Bestimmungen über Standort- und Verkehrsdaten in den Mitgliedsstaaten untersuchen soll. Im Angesicht der starken und wachsenden wirtschaftlichen Interessen an der Nutzung von Standortdaten und den Interessen des Sicherheitsbereichs am Zugriff auf solche Daten kommen hier erhebliche Anstrengungen auf Datenschützer zu, um angemessene Schutzregeln bei der Verarbeitung von Standortdaten zu erreichen.

1 Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation

2 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

3 Artikel 9 der Richtlinie 2002/58/EG

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

5 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden

6 Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12 Digital Rights Ireland und Seitlinger u.a.

7 DRIPA – Data Retention and Investigatory Powers Act 2014, http://services.parliament.uk/bills/2014-15/dataretentionandinvestigatorypowers.html

8 https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/Home/EDPS/Publications/AR

9 Kai Biermann, Was Vorratsdaten über uns verraten, ZEIT Online, 24. Februar 2011, http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz

10 Patrick Beuth, Politiker visualisieren ihr Leben mit Metadaten, ZEIT Online, 27. April 2014, http://www.zeit.de/digital/datenschutz/2014-04/vorratsdatenspeicherung-schweiz-daenemark-visualisierung

11 http://www.d4d.orange.com/en/home

12 http://www.unglobalpulse.org/

13 Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel: Unique in the Crowd: The privacy bounds of human mobility, Nature, March 2013, http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

14 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11, 25. Januar 2012

15 Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket vom 7. März 2012, Randnummer 105, https://secure.edps.europa.eu/EDPSWEB/edps/Consultation/Reform_package

16 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordentliches Gesetzgebungsverfahren: erste Lesung)

17 Studie über die E-Datenschutzrichtlinie: Bewertung und Umsetzung, Wirksamkeit und Kompatibilität mit der vorgeschlagenen Datenschutzverordnung (SMART 2013/0071), Auftragsvergabe 19. April 2014, http://ausschreibungen.dgmarket.com/tenders/np-notice.do?noticeId=10889647



Standorterfassung auf einer Mautbrücke

Tobias Jacquemain

Auf Reisen oder im Alltag: Videoüberwachung in Taxen

Im Licht wachsender Mobilität ist und bleibt das Taxi ein häufig genutztes Transportmittel. Gerade im Urlaub, aber ebenso im Alltag wird auf den Transfer mit Taxen zurückgegriffen. Verlässt man auf Reisen den Flughafen oder Bahnhof, die national wie international von einer weitreichenden Videoüberwachung geprägt sind, erwartet man beim Einstieg in ein Taxi wieder einen diskreten Raum, in dem der Schutz der Privatsphäre mehr Gewicht erhält. Doch wachsende Ansprüche an die dortige Sicherheit und die zunehmende technische Praktikabilität führten in junger Vergangenheit zu einem vermehrten Einsatz von Videoüberwachung im Taxiinnenraum. Ein Raum, der selbstverständlich auch den grundrechtlichen Schutz des Privaten gewährleisten muss, sich aber bei seiner datenrechtlichen Betrachtung von dem bei Videoüberwachung in Bussen und Bahnen unterscheidet. Der Rechtsform der Taxiunternehmer entsprechend fällt der Taxiinnenraum rechtlich unter den nicht-öffentlichen Bereich. Der Staat gewährleistet zwar primär den vom Grundgesetz ausgehenden Schutz der Grundrechte der Bürger gegenüber der von ihm ausgehenden Hoheitsgewalt (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG; § 1 Abs. 2 Ziff. 1, 2 BDSG). Zudem besteht aber auch noch eine Schutzpflicht des Staates[1] für solche Verhältnisse wie im Taxi: Zwischen Bürgern und Privaten muss der Staat die Rahmenbedingungen für eine Einhaltung der grundrechtlichen Verpflichtungen herstellen. Private Datenverarbeiter sind überdies unmittelbar durch das Bundesdatenschutzgesetz (§ 1 Abs. 2 Ziff. 3 BDSG) zur Gewährleistung der Grundrechte der Bürger verpflichtet, wodurch der Bürger in seinem Persönlichkeitsrecht insgesamt umfassenden Schutz genießt.

Zu beachten sind bei der Aufzeichnung eines Innenraums im Taxi in jedem Fall die Rechtsfragen über die grundsätzliche Zulässigkeit, den Umgang mit den gewonnenen Daten und die Anforderung an die Transparenz der Überwachung. Neben diesen auf den spezifischen Sachverhalt abzielenden Rechtsfragen bleiben die damit verbundenen rechtlichen Aspekte bezüglich der grundsätzlichen Zulässigkeit der Überwachung des Fahrers, der nicht selbstständig tätig ist, sondern als Arbeitnehmer in einem größeren Taxiunternehmen angestellt ist, und welche Rechtsfolgen bei Verstößen gegen Datenschutz zu erwarten sind, bestehen, werden jedoch mangels eigener Spezifik im Folgenden nicht weiter behandelt. Zu bedenken ist schlicht, dass es Taxifahrer gibt, die nicht mit dem Taxiunternehmer identisch sind, und demnach datenschutzrechtlich als Arbeitnehmer zu behandeln sind. Der Frage über die Zulässigkeit der Überwachung im Taxi ist insbesondere unter Würdigung des Gebots der Verhältnismäßigkeit mit einer intensiven Prüfung der Alternativen zu begegnen. Sprechen wir über Datenschutz bei Reisen, sollen Eindrücke aus anderen EU-Mitgliedstaaten als Reiseziele der Deutschen nicht unberücksichtigt bleiben. Einem über die Grenzen der EU hinausgehenden Vergleich ist aufgrund der weltweiten Präsenz von Taxen nicht Herr zu werden und dieser bleibt daher unversucht.

Das stets von Taxiverbänden und -vereinigungen zu Recht vorgebrachte Sicherheitsbedürfnis zielt lediglich auf den Schutz des Taxifahrers ab. Der Fahrgast kann durch eine Kamera im Besitz des Fahrers beim Einstieg in dieses Transportmittel keinen höheren Schutz genießen, was man noch als Service im Sinne des Gastes verstehen könnte; schließlich kann der Taxifahrer nach jeder begangenen Straftat sämtliche Daten theoretisch wieder verschwinden lassen. Das vorgebrachte Sicherheitsbedürfnis ist aber vom Ausgangspunkt her bereits fragwürdig, wenn man die Statistik des Jahres 2012 für Frankfurt, immerhin die an der Einwohnerzahl gemessen fünftgrößte Stadt Deutschlands, betrachtet, wonach „7 Raubstraftaten zum Nachteil von Taxifahrern und Taxifahrerinnen“[2] im gesamten Jahr bei der Polizei gemeldet wurden. Gleichwohl sind Serien von Gewalttaten gegen Taxifahrerinnen und -fahrer auch in Kleinstädten immer wieder ein Thema in den Medien.

Stellt man sich die Frage, inwieweit die Videoüberwachung in Taxen überhaupt rechtlich gangbar ist, muss diese zunächst abgegrenzt werden von sog. Unfallkameras („dashcams“). Diese ebenfalls im Innenraum von Kraftfahrzeugen montierten Kameras zeichnen während der Fahrt den öffentlichen Raum auf und sind in keiner Weise mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar. Zielt die technische Vorkehrung allerdings auf die visuelle Kontrolle des Bereichs ab, in dem der Fahrgast Platz genommen hat, bedarf es der Abwägung der Interessen zwischen Fahrer und Fahrgast: Ersterer hat das Schutzbedürfnis respektive seiner Unversehrtheit und seines Besitzes vorgebracht, letzterer legt Wert auf die Wahrung seiner vom Grundgesetz garantierten Persönlichkeitsrechte. Gesetzlich geregelt ist die etwaige Videoüberwachung im BDSG in § 6b „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen“, wonach die Zulässigkeit bei der „Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ (§ 6b Abs. 1 Nr. 3 BDSG) gegeben ist. Schranken erhält dieses Gebot allerdings in Absatz 3: Demnach muss das Kriterium für die Erforderlichkeit die Videoüberwachung betreffend gegeben sein und das Schutzbedürfnis des Fahrgastes darf nicht überwiegen. Für den praktischen Vollzug hat der Düsseldorfer Kreis (DK) als Ergebnis der Abwägung zwischen den konträren Interessen im vergangenen Jahr auf Initiative des Landesbeauftragten für



Bild: RainerSturm – pixelio.de

Datenschutz und Informationsfreiheit Nordrhein-Westfalen einen Beschluss[3] gefasst, der permanente Videoüberwachung im Innenraum des Wagens nicht gestattet. Der Beschluss stellt klar, dass dortige Aufzeichnungen nicht unter die Wahrnehmung des Hausrechts fallen, wie man auch hätte argumentieren können, sondern es bedarf zur Erlaubnis der Festlegung eines konkret festgelegten Zweckes. Darin schließt sich die Frage an, ob hierfür eine „generellen Gefahrenlage“ ausreicht oder es einer „hinreichend konkretisierten Gefahrensituation“ bedarf, wie es u. a. das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) verlangt.[4] Der Grundsatz der Erforderlichkeit und der Verhältnismäßigkeit ist in jedem Fall zu beachten. Demzufolge vorzuziehen sind solche Überwachungsinstrumente, die die Rechtsfigur des Fahrgastes weniger beeinträchtigen. Beispielhaft nennt der DK hier einen „stillen Alarm“ oder Notrufsignal mit GPS-Ortung. Das ULD ergänzt diese um ebenfalls leicht realisierbare Schutzmöglichkeiten wie die mechanische Absicherung des Fahrerbereichs und die Verwendung eines abschließbaren sicheren Faches für Bargeld und Ähnliches. Erst bei Berücksichtigung dieser Schutzmöglichkeiten sind Videoüberwachungen denkbar. So sind auch dann Standbilder beim Einsteigen oder Aufzeichnungsfrequenzen von maximal 15 Sekunden im Sinne der Verhältnismäßigkeit und Erforderlichkeit vorzuziehen, so der DK. Zudem könnte ein Taxifahrer bei der situativen Einschätzung einer Gefahr eine installierte Kamera offen erkenntlich aktivieren und damit eine länger andauernde Aufnahme beginnen. Unabhängig von der tatsächlichen Nutzung verlangt das Gebot der Transparenz die Kenntlichmachung mithilfe von Piktogrammen oder Schildern, die auf eine im Auto installierte Videokamera vor dem Einstieg hinweisen (§ 6b Abs. 2 BDSG). Mithin muss ebenfalls die verantwortliche Stelle benannt sein. Somit stimmt der Fahrgast beim Einstieg lediglich dem Umstand zu, dass ausgehend von einer vorhandenen technischen Installation eine Videoaufzeichnung geschehen könnte, allerdings nur in einem zum vorab festgelegten Zwecke erforderlichen Fall. Unter Würdigung der Persönlichkeitsrechte der Fahrgäste gilt: „Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig.“[5]

Erwartungsgemäß reicht dieser Beschluss den deutschen Taxifahrern nicht weit genug. Damit würde das System „torpediert“ und nach ihren Vorstellungen wäre es in einer tatsächlichen Notsituation gar nicht mehr möglich einen Notknopf zu drücken.[6] Auch wenn man anerkennen muss, dass der Interessenverband das Thema Datenschutz im Zusammenhang mit der Videoüberwachung bereits seit den 1990er Jahren bearbeitet, sind die Fronten verhärtet, wenn der Verbandspräsident behauptet: „Datenschutz darf nicht unsere Sicherheit gefährden!“[7]

Was passiert mit den gewonnen Daten? Im Regelfall sind diese nach 24 Stunden, maximal aber 48 Stunden später zu löschen, wenn die Fahrt ereignislos endete. Demnach könnte man – auch im Sinne des Gebots der Zweckbindung bei der Datenerhebung – die Daten theoretisch auch unmittelbar nach Ende der Fahrt löschen. Der Fahrer und sein Fahrzeug hätten die Fahrt schließlich unversehrt überstanden, womit keine Rechtfertigung für die weitere Speicherung mehr vorliegt.

Zusammenfassend lässt sich für den deutschen Rechtsraum festhalten, dass eine Videoüberwachung innerhalb von Taxen nur unter vorheriger Ausschöpfung zahlreicher Alternativen zu installieren ist und die eigentliche Nutzung einer tatsächlich zugrundeliegenden Gefahrensituation bedarf, womit eine unbegründete Dauernutzung nicht gestattet ist. Zumindest in der theoretischen Betrachtung sind die Persönlichkeitsrechte der Kunden nur weniger beeinträchtigend berührt als eine grundlose Daueraufnahme während der Fahrt es befürchten lässt. Zudem ist es fragwürdig, ob Videoüberwachung grundsätzlich Schaden vom Fahrenden abwenden kann. Die abschreckende Wirkung mag in Maßen bestehen, doch ist der Schaden erst eingetreten, lässt sich dieser durch

eine Videoaufzeichnung gewiss nicht lindern und garantiert ebenso wenig den Erfolg bei der Strafverfolgung.

Blickt man über die Landesgrenzen hinweg zu möglichen Reisezielen in der europäischen Rechtsgemeinschaft, eröffnet sich ein ähnliches Bild. So ist in Italien einem Beschluss der dortigen Datenschutzbehörde aus dem Jahr 2010 zufolge detailliertes Filmen im Taxi grundsätzlich nicht nach den dortigen Datenschutzbestimmungen zulässig. Videoüberwachung ist dort analog zu den deutschen Bestimmungen unter Einhaltung der Datenschutzprinzipien – Datensparsamkeit bei der Erhebung, Verhältnismäßigkeit und Zweckbestimmung – erlaubt, sofern von außen auf die Videoinstallation visuell hingewiesen wurde.[8] Die Bestimmungen seitens des irischen Datenschutzes sind annähernd gleichlautend.[9] Sie grenzen sich nur darin von deutschen Regelungen ab, dass hier alternative Sicherheitsvorkehrungen, die das Grundrechte der Fahrgäste auf Privatsphäre weniger beeinträchtigen, auszuschöpfen und zu bevorzugen sind, bis letztlich auf die Aufnahme von Bildmaterial zurückgegriffen wird.

Positiv hervorzuheben sind die italienischen Bestimmungen, die im Sinne des Arbeitnehmerdatenschutzes die permanente Überwachung des Fahrers explizit verbieten.[10] So wie eine solche Videoüberwachung in Deutschland nicht von § 32 BDSG gedeckt wäre, erlaubt das italienische Recht dieses Vorgehen zur Sammlung relevanter Leistungsdaten des Arbeitnehmers ebenfalls nicht.

Begibt man sich für eine Dienst- oder Urlaubsreise in die Metropole London, sinkt die Sensibilität im Umgang mit den Daten spürbar. Zwar ist mit Piktogrammen vor dem Einsteigen auf etwaige Kameras hinzuweisen, doch innerhalb des Taxis ist die Gewinnung von permanenten Bewegtbildern ohne Weiteres gestattet. Selbst die Tonaufnahme ist, wenn auch unter hohen Anforderungen, rechtlich zulässig. Die so gewonnen Daten dürfen bis zu 31 Tage nach Aufnahme bei der verantwortlichen Stelle gespeichert bleiben; erst dann sind sie verpflichtend zu löschen.[11] Auch die dort explizit benannten Gründe für die Videoüberwachung, die neben dem üblichen Schutz vor Gewalt auch das „Gefühl der Abwesenheit von Angst“ beinhalten, aber vor allem die Unterstützung der Polizei und Versicherungen bei der Aufklärung von Verbrechen und Unfällen nennen, rechtfertigen kaum diese lange Speicherfrist. Zum Vergleich: Die vom irischen Datenschutzbeauftragten benannte Speicherfrist beläuft sich auf maximal 24 Stunden.

Mit Blick auf die Verhältnisse in Spanien fällt auf, dass die staatliche Seite auch eine große Rolle bei der organisatorischen Realisierung der Videoüberwachung in Taxen spielen kann. So ist dort die Videoüberwachung unter Achtung der fundamentalen Persönlichkeitsrechte der Fahrgäste grundsätzlich zulässig, doch bis zur Benutzung einer solchen technisch Vorrichtung sind eine Reihe bürokratischer Hürden zu meistern: Die technische Installation einer Kamera ist ausschließlich von privaten Sicherheitsfirmen vorzunehmen, die dafür jeweils eine Erlaubnis von spanischen Innenministerium einholen müssen. Sollten die Daten zudem gespeichert werden, muss das Taxiunternehmen dies der nationalen Datenschutzbehörde vorher melden und sich in ein dort geführtes Register videoüberwachender Unternehmen eintragen.[12]

Abschließend lässt sich festhalten, dass der deutsche Rechtsrahmen den Videoaufzeichnungen im Taxi sehr enge Grenzen setzt. Gleichwohl bleibt aber auch die Aufnahme von Standbildern oder kurzen Sequenzen ein, wenn auch maximal geringer, Eingriff in die Privatsphäre, der aus Gründen des Sicherheitsbedürfnisses der Personenbeförderer erlaubt wird. In der Praxis lässt sich bei individueller Wertschätzung für höheren Datenschutz ein Taxi, das ohne Videokamera ausgestattet ist, bevorzugen und somit das Problem umgehen. Problematisch wird es erst in Städten wie Remscheid, die möglicherweise bereits Zukunftsszenarien repräsentieren, in denen ausnahmslos alle Taxen mit der Überwachungsmöglichkeit technisch ausgerüstet sind und davon entsprechend Gebrauch machen.[13] Die größte Gefahr besteht aber in einer gesetzlich nicht erlaubten Dauerüberwachung von Fahrern als Arbeitnehmern und deren Fahrgästen, die unbemerkt erfolgt, weil sie technisch so leicht möglich ist.

1 Kotzur, ZRP 2013, 216, 217.

2 Polizeipräsident Frankfurt, Antwort auf Anfrage der „ELF Piraten Fraktion“, 2013, http://elf-piraten.de/downloads/taxigewalt-polizeipraesidium-2013-06-11.pdf.

3 Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis): Videoüberwachung in und an Taxis, 2013, https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2013/Videoueberwachung_in_und_an_Taxis/Video__berwachung_in_und_an_Taxis.pdf.

4 ULD-SH, Videoüberwachung an und in Taxis, 2012, https://www.datenschutzzentrum.de/video/20120112-videoueberwachung-taxis.html.

5 ULD-SH, Fn. 4.

6 Deutscher Taxi- und Mietwagenverband e.V. (BZP), BZP-Report 3/2013, 1, http://www.bzp.org/Content/INFORMATION/BZPReport/2013/doc/BZP_Report_2013_Heft_3.pdf.

7 BZP-Präsident Michael Müller, BZP-Report 3/2013, Fn. 6.

8 Italienische Datenschutzbehörde („Garante per la Protezione dei Dati Personali“), Videoüberwachung: Beschluss vom 8. April 2010, Ziff. 4.4.2. f., http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680.

9 Irischer Datenschutzbeauftragter („Data Protection Commissioner – Ireland“), Nutzung von Videoüberwachung („Use of CCTV“), http://www.dataprotection.ie/docs/CCTV/1242.htm#5.

10 Italienische Datenschutzbehörde, Fn. 8, Ziff. 4.1 i. V. m. Ziff. 4.4.

11 Der Bürgermeister von London, Guidelines for CCTV Systems in licensed London Taxis & Private Hire Vehicles, 2011, http://www.tfl.gov.uk/cdn/static/cms/documents/cctv-guidelines-for-taxis-and-phvs.pdf; i. V. m.: Datenschutzbehörde von Großbritannien (“Information Commissioner´s Office), CCTV code of practice, 2008, http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf.

12 Spanische Datenschutzbehörde („Agencia Española de Protección de Datos“), Videoüberwachung in Taxen, Information 0365/2007.

13 Voregger, „Foto-Fix im Taxi: Videoüberwachung auf vier Rädern“, SPIEGEL ONLINE 29.10.2002, http://www.spiegel.de/netzwelt/web/foto-fix-im-taxi-videoueberwachung-auf-vier-raedern-a-220197.html.

Interview mit Thilo Weichert

Gläserne Touristen zwischen Big Data und Staatsüberwachung

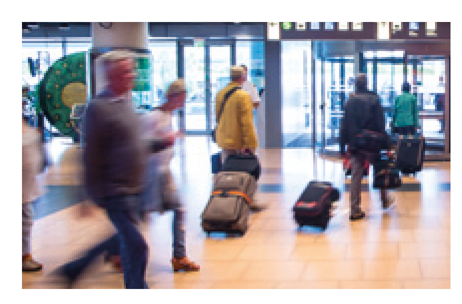


Bild: Rainer Sturm – pixelio.de

Jede Reisebuchung, jede Internetsuche nach Reisezielen und Unterkünften und jedes elektronische Bezahlen führt zu digitalen Spuren. Die Daten werden in privaten und staatlichen Datenbanken zusammengeführt und mit Data-Mining- und Big-Data-Werkzeugen ausgewertet. Damit werden Milliarden umgesetzt. Vordergründiger Zweck ist z. B. die Vereinfachung künftiger Netzsuchen durch gezielte Vorschläge gemäß dem persönlichen Nutzungsprofil. Die Effekte können aber auch für die Betroffenen desaströs sein, wenn die detailreichen individuellen Profile von uns manipulativ oder diskriminierend oder gar für kriminelle Zwecke genutzt werden. Die Tourismusindustrie verspricht sich von „gläsernen Touristen" unter Einsatz von Big Data steigende Umsätze, Behörden erhoffen sich mehr Sicherheit. Für Datenschützer sind die Verarbeitungsprozesse ein bisher wenig transparent gemachtes Risiko. Viel zu wenig ist bekannt, wer welche Daten für welche Zwecke nutzt und damit möglicherweise viel Geld verdient.

Frage: Bei Online-Buchungen werden jede Menge Informationen eingefordert, ebenso wie im Laufe einer Reise. Reisekonzerne, Werbefirmen und Internetportale verknüpfen diese Informationen zu umfassenden Datenprofilen. Was bringt Big Data den Touristen?

Weichert: Big Data ist Verheißung und Bedrohung zugleich, je nachdem, was die Datenverwerter im Schilde führen und was die Kunden erwarten. Für viele ist ein individuell zugeschnittenes Reiseangebot ein Segen und eine Entscheidungshilfe; für andere ist es eine Zumutung, weil man bei der Urlaubsplanung und -durchführung entmündigt wird. Richtig ärgerlich wird Big Data, wenn das Ergebnis ist, dass das Angebot deshalb teurer bzw. nachteiliger ausfällt, weil die Big-Data-Datenauswertung zum Ergebnis kommt, dass ein Kunde nicht auf den Preis schaut, kein Auge für Qualität hat oder – noch schlimmer – sich voraussichtlich bei einer mangelhaften Leistung nicht zur Wehr setzen wird oder kann.

Frage: Die Touristikbranche behauptet, mit Big Data würden Reisende auf sie persönlich zugeschnittene Angebote erhalten, was für diese nur nützlich sei?

Weichert: Big Data bedeutet zunächst nicht Selbstbestimmung, sondern Fremdbestimmung – beginnend bei der Werbeansprache, über die Preis- und Vertragsgestaltung bis hin zur Vertragsabwicklung. Wer persönlich zugeschnittene Angebote haben möchte, der soll dies bekommen. Voraussetzung ist aber, dass er dem zuvor zugestimmt hat, er also insofern sein Selbstbestimmungsrecht an den Anbieter delegiert hat. Die Wirtschaft generell und der Tourismussektor speziell arbeiten aber leider zumeist nicht einwilligungsbasiert, sondern – teilweise sogar mit dem Segen des Gesetzes – im Dunkeln für die Betroffenen. Bei deutschen Anbietern kann man noch davon ausgehen, dass diese sich einigermaßen an die gesetzlichen Regelungen halten. Das ist bei ausländischen Unternehmen nicht so sicher, insbesondere bei US-Portal- und -Werbeanbietern, die bis vor kurzem meinten, sie müssten sich überhaupt nicht an unserem Recht orientieren.

Frage: Neben Wirtschaftsunternehmen interessieren sich auch staatliche Stellen, insbesondere Sicherheitsbehörden, für die Daten. Was hat dies für Konsequenzen?

Weichert: Eine datenschutzrechtliche Katastrophe ist aus meiner Sicht die insbesondere von den USA aber auch z. B. von Großbritannien praktizierte Überwachung des Flug- und Schiffsverkehrs und die Totalüberwachung von internationalen Banktransaktionen. In den USA läuft das unter den Begriffen „Passenger Name Record Program" und „Terrorist Finance Tracking Program". Dabei werden unter dem Vorwand der Terrorismusbekämpfung sämtliche Menschen, die international unterwegs sind, durchleuchtet. Ein weiteres, bisher viel zu wenig bewusstes und kontrolliertes Thema ist der Zugriff von Sicherheitsbehörden auf die Hotel- und Reisebuchungsprogramme der Anbieter – online wie offline. Bei Internet-Buchungen haben viele, nicht nur die NSA, einen direkten Zugriff auf die Daten. Bei geschlossenen internationalen Systemen wie z. B. „Amadeus" dürfte dies ebenso sein. Bei regionalen Anbietern dürfte dagegen der Zugriff auf die internen Buchungssysteme durch Behörden nicht ganz so einfach sein.

Frage: Was droht Reisenden, die zu viele Daten preisgeben?

Weichert: Denkbar ist vieles: Wer in sozialen Netzwerken allgemein zugänglich herausposaunt, dass zu Hause niemand nach dem Rechten schaut, lädt geradezu Einbrecher ein. Wer bei unzuverlässigen Akzeptanzstellen elektronisch bezahlt, muss befürchten, dass das Giro- oder Kreditkartenkonto geplündert wird. Wer auf Seiten im Internet unterwegs ist, über die viele Werbecookies gesetzt werden, der wird mit Online-Werbung zugeschüttet. Wer mehr Daten als für einen Dienst nötig offenbart, muss befürchten, dass diese Daten zweckfremd weiterverwendet werden...

Frage: Was gibt es als Gegenleistung?

Weichert: Generell gilt: Es dürfen nur die Daten eingefordert werden, die für einen Service unbedingt gebraucht werden. Bei touristischen Apps können dies auch schon mal Lokalisierungsdaten sein. In jedem Fall sollte den Nutzenden jeweils transparent gemacht werden, welche Daten benötigt und für welche Zwecke diese genutzt werden. Bei einer zweckändernden Nutzung, z. B. für Werbezwecke, müsste hierauf hingewiesen werden und darauf, dass man dieser Nutzung widersprechen kann. Die Realität bleibt insofern oft weit hinter dem Gesetz zurück. Ob sich die Datenpreisgabe lohnt, muss jeder Einzelne selbst entscheiden. Leider erkennen wir das aber erst viel zu spät, insbesondere, wenn es sich nicht gelohnt hat.

Frage: Gibt es Services, mit denen ich meine Daten geschützt in der Urlaub mitnehmen kann, z. B. Reisepass- und Ausweis-Kopien oder Krankenversicherungsdaten?

Weichert: Ich kann und will keine Empfehlungen geben angesichts der gewaltigen Masse von Applikationen auf dem Markt. Bisher ist mir keine bekannt, die förmlich auf ihre Datenschutzkonformität hin überprüft und zertifiziert worden wäre. Kontrollierte Zertifizierungsverfahren, die von der D21-Initiative anerkannt sind, gibt es für Online-Shops, auch im Tourismusbereich. Sinnvoll ist in jedem Fall die Recherche im Netz und das Studium von vergleichenden Studien in Verbraucherzeitschriften. In jedem Fall sollten, wenn ich meine Daten elektronisch mit mir führe, diese gut verschlüsselt gespeichert werden. Sonst läuft man Gefahr, dass bei einer Gepäckkontrolle der Laptop, das Smartphone oder das sonstige IT-Gerät mal kurz auf seinen gesamten Inhalt hin überprüft wird und der gesamte Datenbestand in den Rechenzentren von neugierigen Geheimdiensten landen. Dass dies bei einigen Ländern passiert, ist uns wieder durch Edward Snowden in Erinnerung gebracht worden.

Frage: Welche Daten sollte man für sich behalten?

Weichert: Insofern sind die Schmerzgrenzen sehr unterschiedlich. Gesundheitsdaten, Lokalisierungsdaten sowie Daten aus meinem privaten und familiären Umfeld sind für mich persönlich absolut tabu. Bei Bank- und Kreditkartendaten bin ich äußerst vorsichtig und versuche deren Offenbarung zu vermeiden, z. B. indem ich bar und im Hotel vorab bezahle. Meine Adressdaten sowie sonstige identifizierenden Angaben muss ich oft zwangsläufig offenbaren, z. B. beim Einchecken in ein Hotel.

Frage: Wie praktiziere ich im Urlaub Datensparsamkeit?

Weichert: Datensparsamkeit ist manchmal in der Praxis schwierig. Oft wird fälschlich behauptet, bestimmte Angaben seien für einen Service unabdingbar. Lehnt man dann den Service mit dem Argument fehlender Erforderlichkeit ab, geht es sehr oft auch ohne. Wer sich nicht auf leidige Datenschutzdebatten mit seinen Gegenübern einlassen möchte, der kann und sollte es sich angewöhnen, falsche oder Pseudonymdaten anzugeben. Doch Vorsicht: Derartiges kann nach hinten losgehen, etwa wenn man eine Reklamation vorbringen will und nicht beweisen kann, dass man selbst der Vertragspartner ist.

Frage: Was ist zu beachten?

Weichert: Wer ohne Begründung mehr Daten einfordert als für mich persönlich plausibel ist, dem sollte ich mich nicht anvertrauen. Entsprechendes gilt, wenn sonstige Hinweise auf die fehlende Seriosität oder gar auf einen kriminellen Hintergrund bestehen.

Frage: Was ist von den Plänen der IATA zu halten, Passagiere künftig beim Check-In nach bekannten und bedrohlichen Passagieren zu trennen? Kann dann z. B. Kritik an der US-Regierung auf einer Facebookseite zu einem Einreiseverbot führen? http://www.iata.org/whatwedo/security/Pages/smart-security.aspx

Weichert: Diese Pläne sind sehr dubios. Deren Umsetzung dürfte nicht vereinbar sein mit unserem freiheitlichen Menschenbild, wonach niemand wegen bestimmter Merkmale oder auf Grundlage reiner Verdächte diskriminiert werden darf. Wir müssen aber leider zur Kenntnis nehmen, dass viele Staaten und insbesondere die USA genau das schon praktizieren, indem sie nach unbekannten Kriterien Leute auf sog. No-Fly-Listen setzen. Das hat anscheinend immer wieder als Hintergrund, wie sich jemand politisch betätigt oder geäußert hat. Eine solche Praxis ist meines Erachtens undemokratisch und rechtsstaatswidrig.

Frage: Was bringt die digitale Zukunft noch so alles für Touristen?

Weichert: Die Zukunft steht – wie es so schön heißt – in den Sternen. In ihr wird es einen Flickenteppich unterschiedlichster Überwachungs- und Verarbeitungspraktiken geben. Ob die Reisenden zu Konsumtrotteln mit digitalen Vollprofil degradiert oder als selbstbestimmte Verbraucher behandelt werden, das hängt nicht zuletzt auch von uns, also von jedem selbst, ab. Wichtig ist aber in jedem Fall, dass die Rahmenbedingungen stimmen, also ob es Datenschutzgesetze gibt, die auch durchgesetzt werden, und ob es in der Gesellschaft eine anerkannte Datenschutzkultur gibt.

Frage: Welche Stellen aus der Reisebranche verarbeiten welche Daten?

Weichert: Generell gilt, dass sämtliche Vertragsdaten gespeichert werden und zwar sowohl von den Dienstleistern, also etwa Flug- oder Bahngesellschaft und Hotel, über den Reiseveranstalter bis zum Reisebüro. Anstelle des Reisebüros kann der Betreiber eines Online-Portals treten. Eingebunden können weitere Anbieter sein, also z. B. Versicherungen, Autovermieter, Eventveranstalter. Bei Online-Buchungen kommt noch die gesamte Internet-Branche mit den Nutzungsdaten hinzu. Für die Branche spannend sind sämtliche Internet-Kommentare zum Angebot, aber auch die Eintragungen zu den jeweiligen Kunden. Relevant sind weiterhin Abwicklungsangaben, also Zahlungsdaten, aber etwa auch Angaben zu Beschwerden und Konflikten. Sensible Angaben, etwa zu Gesundheit, zu politischen oder religiösen Anschauungen oder zu sexuellen Präferenzen sind bei einzelnen Angeboten möglicherweise relevant. In diesem Fall benötigt die verantwortliche Stelle aber für die Verarbeitung eine besondere Legitimation, zumeist also eine explizite Einwilligung.

Stephan Möhrle

Drohnen – „fliegende Augen“ und Datenschutz

Rechtliche Aspekte zur Verwendung „unbemannter Luftfahrzeuge“



Bewaffnete militärische Drohne vom Typ MQ-1 Predator. Bild: Frans Jozef Valenta

In Deutschland wurde ein Gesetz geschaffen, um den Umgang mit zivilen Drohnen zu regeln, aber tatsächlich ist der Regelungsgehalt des Gesetzes denkbar gering. Eine Debatte über die datenschutzrechtlichen Bedenken gegen die durchaus als Überwachungsgeräte einsetzbaren Micro-Air-Vehicles (MAV) gab es gleich gar nicht.

Beginnen wir jedoch etwas früher: Im Kosovokrieg 1998/99 setzte die Bundeswehr erstmals unbemannte Luftaufklärungsdrohnen – damals die CL-289 – ein. Seither sind unbemannte Luftfahrzeuge ein Thema von wachsendem Interesse. Seit 2004 ist bekannt, dass die Schweizer Armee bei Trainingsflügen mit Aufklärungsdrohnen – in diesem Fall mit dem Aufklärungsdrohnensystem 95, kurz ADS-95, ein vom Konzern Ruag in der Schweiz in Kooperation mit Israel Aircraft Industries gefertigtes Aufklärungssystem – zufällig ausgewählte Privatautos und Zivilpersonen filmte, wie eine Fragstunde im Schweizer Parlament auf Anfrage der Abgeordneten Boris Banga und Hans Widmer zu Tage förderte. In der Schweiz schloss sich, anders als in Deutschland, an diese Erkenntnis eine öffentliche Diskussion über die zentralen Fragen des Datenschutzes an. Einer breiten Öffentlichkeit ist das Problem der unbemannten, aber bewaffneten Luftfahrzeuge spätestens seit den „gezielten Tötungen“ der US-amerikanischen Streitkräfte im „Krieg gegen den Terror“ bekannt.

Während sich bei der Kriegsführung mit Drohnen eine rechtlich durchaus diffizile Fragestellung ergibt, die nicht ohne Weiteres seitens einzelner Nationalstaaten gelöst werden kann, könnte bei den Fragen, die sich mit der Nutzung von Drohnen durch nationale Sicherheitsbehörden und durch Private beschäftigt, zumindest im Rahmen von innerstaatlichem Recht eine Reglementierung stattfinden.

In Niedersachsen und Sachsen nutzt die Polizei bereits Drohnen zur polizeilichen Aufklärung. An den Universitäten Siegen, Paderborn und Dortmund gibt es das „AirShield-Programm“, das mit Gasmessgeräten ausgestattet ist und bei Katastrophen von Feuerwehren oder dem Technischen Hilfswerk eingesetzt



Diehl BGT defence Minihubschrauber für militärische und zivilstaatliche Einsätze.
Bild: Stahlkocher – Mario Link.
Lizenziert unter Creative Commons Attribution-Share Alike 3.0 über Wikimedia Commons

werden soll. Amazon hat angekündigt, dass es unter der Bezeichnung „Prime-Air" die Auslieferung von Bestellungen mit Drohnen bereits für das Geschäftsjahr 2014 plant. Fast zeitgleich hat die Deutsche Post AG ebenfalls den Einsatz von „Paketkoptern" für besonders eilige Sendungen angekündigt.

„Die Schlagkraft der Truppe"

In Deutschland wird die Nutzung von Drohnen seit der Neuordnung in der Luftverkehrsordnung (LuftVO) und dem Luftverkehrsgesetz (LuftVG) geregelt. Dieses bestimmt, dass unbemannte Luftsportsysteme unter fünf Kilogramm, die zur reinen Freizeitnutzung betrieben werden, keine Aufstiegsgenehmigung brauchen. Allerdings können diese zum Teil sehr leistungsfähigen Geräte mit Kameras ausgestattet werden und so zu „fliegenden Augen" werden.

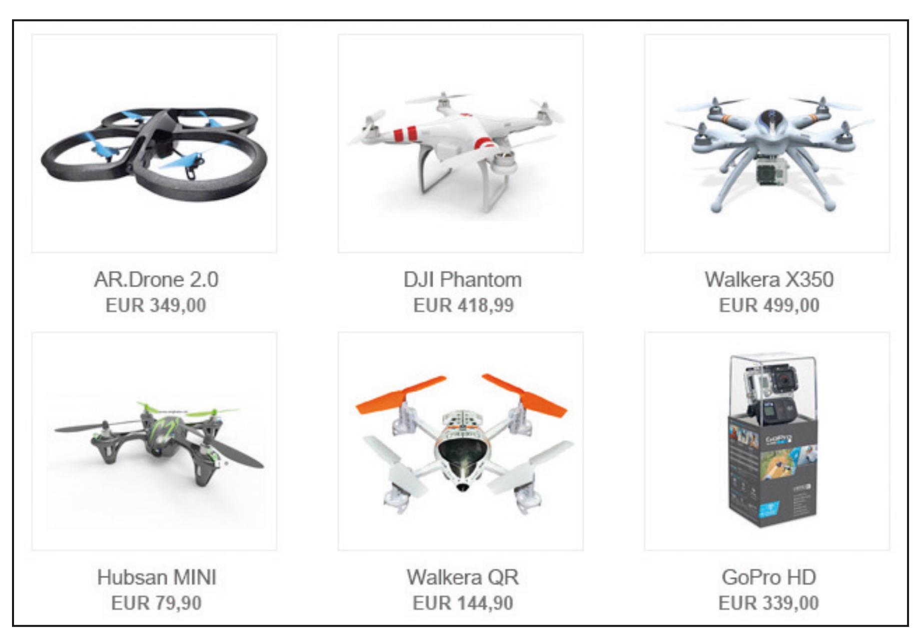
Da Drohnen immer preiswerter werden und zunehmend einfacher zu bedienen sind, stellt sich die Frage nach dem besonderen Schutzbedürfnis des Einzelnen gegen dadurch möglich werdende Eingriffe in den höchst persönlichen Lebensbereich. Leider hat es der Gesetzgeber versäumt, diese Eingriffe separat zu sanktionieren. So bleibt bei den sich aufzwingenden Fragen zu Überwachungs- und Fotodrohnen im privaten Bereich nur, auf die bereits bestehenden zivil- und strafrechtlichen Grundlagen zu verweisen, wie sie für Fotoaufnahmen gelten, und diese entsprechend anzuwenden. Grundsätzlich sind bei Fotoaufnahmen mit Drohnen die Urheberrechte eines Architekten an seinen Bauwerken zu beachten. In diese Rechte wird durch eine Ablichtung auch aus der Bordkamera einer privaten Drohne eingegriffen. Soweit diese Bilder aber nur im rein privaten Umfeld verwendet werden, ist dies rechtlich unbedenklich.

Anders sieht die Rechtslage allerdings aus, wenn die Bilder im Internet oder an anderer Stelle öffentlich zugänglich gemacht werden. Im Normalfall gilt zwar bei Aufnahmen von Gebäuden die Panoramafreiheit. Demnach darf ein Foto eines an einer öffentlichen Straße oder einem öffentlichen Platz stehenden Bauwerks verbreitet werden, wenn es sich auf die Ansicht beschränkt, die von der Straße oder dem Platz aus zu sehen ist. Anders sieht das mit der Veröffentlichung der Rückseite und des Innenhofes aus. 2003 hat der Bundesgerichtshof die Panoramafreiheit für Luftaufnahmen in seinem Hundertwasser-Haus-Urteil präzisiert.

Besondere Aufnahmebeschränkungen schafft natürlich der § 109g Strafgesetzbuch, welcher das Fotografieren von militärisch relevanten Bereichen und Geräten verbietet, wenn dadurch „wissentlich die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe gefährdet" wird.

Auch die Abbildung der sich sonnenden Nachbarin ist bereits durch den „Paparazzi-Paragrafen" 201a des Strafgesetzbuchs geregelt. Dieser untersagt Aufnahmen aus dem höchstpersönlichen Lebensbereich einer Person. Hier genügt bereits allein die Herstellung der Bilder. Die Intimsphäre verletzt in diesem Fall derjenige, der Bilder einer anderen Person aufnimmt, die sich in der Wohnung oder einem gegen Einblick besonders geschützten Raum befindet. Im Übrigen steht nicht nur die Herstellung unter Strafe. Wer Bilder zwar mit Einverständnis des Abgebildeten aufnimmt, diese aber ohne oder gegen dessen Wissen an Dritte weitergibt, macht sich ebenso strafbar. In beiden Fällen muss mit einer Geldstrafe bis hin zu einer Freiheitsstrafe von einem Jahr gerechnet werden.

Dieser Artikel erschien in der Zivil-Courage 2/2014; Weitere Materialien sind im Internet abrufbar unter www.dfg-vk.de/dateien/ZC-2013-02-WEB.PDF



Spielzeug-Drohnen mit Kamera werden immer beliebter. Screenshot: http://www.drohne-kaufen.net/

„Freiheit statt Angst“

Demonstration gegen Überwachung am 30.08.2014 in Berlin

Zur Demonstration „Freiheit statt Angst – Aufstehen statt Aussitzen“ rief ein breites zivilgesellschaftliches Bündnis von 81 Organisationen auf, unter anderem der Arbeitskreis gegen Vorratsdatenspeicherung, Amnesty International, die Internationale Liga für Menschenrechte, Digitalcourage, der Verbraucherzentrale Bundesverband, die Neue Richtervereinigung, die Freie Ärzteschaft, Reporter ohne Grenzen, Campact, der Chaos Computer Club und die Deutsche Vereinigung für Datenschutz.

Das Veranstaltungsbündnis freut sich über die gelungene Mobilisierung – mehr als 6.500 Menschen waren in Berlin auf die Straße gegangen und hatten gemeinsam unter dem Motto „Aufstehen statt Aussitzen“ ein Zeichen für Grundrechte und gegen Massenüberwachung gesetzt.



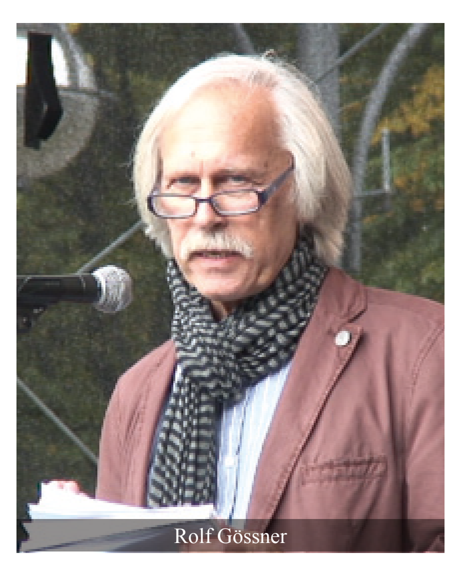
Peter Schaar

„Die generelle, anlasslose Speicherung von Telekommunikationsdaten ist weder mit dem Grundrecht auf Privatsphäre noch mit dem Grundrecht auf Datenschutz vereinbar“, betonte der ehemalige Bundesdatenschutzbeauftragte Peter Schaar und forderte ein komplettes Verbot der Vorratsdatenspeicherung auf EU-Ebene. Peter Schaar sagte weiter: „Es stellt sich die Frage, ob die heute eingeschulte Generation in einer Welt aufwachen wird, die durch totale Überwachung gekennzeichnet ist.“



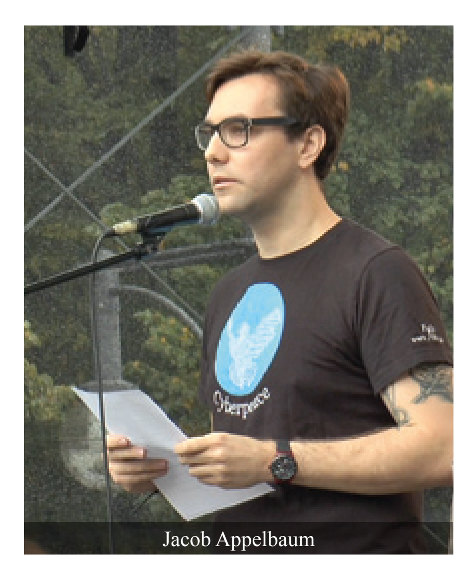
Annegret Falter

Annegret Falter vom Whistleblower-Netzwerk fragte: „Wo bleiben die deutschen Whistleblower?“, und stellte klar: „Entsprechende Gesetzesänderungen sind überfällig! Dann wären Mitarbeiter geschützt, die zu illegalen Machenschaften ihrer Behörde nicht länger schweigen wollen“, und weiter: „Aufrechte Mitarbeiter und Mitarbeiterinnen bei den Behörden, die Unrecht und gefährliche Entwicklungen öffentlich machen, sollen nicht um ihr Wohlergehen fürchten müssen.“



Rolf Gössner

Rolf Gössner, Sprecher für die Internationale Liga für Menschenrechte, beklagte, dass der Generalbundesanwalt auf Ermittlungen wegen Massenüberwachung durch Geheimdienste verzichtet – aus vorgeblichem Mangel an konkreten Hinweisen. „Das ist Realitätsverleugnung hart an der Grenze zur Strafvereitelung im Amt!“ Jubel bekam Gössner für seinen Aufruf zu mehr Whistleblowing und Zivilcourage: „Was wir brauchen: Einen Snowden im BND und im Verfassungsschutz!“ Gössner forderte schließlich die komplette Auflösung der Geheimdienste – eine Forderung, die auf lautstarke Zustimmung der Demonstrierenden stieß.



Jacob Appelbaum

Jacob Appelbaum, amerikanischer Datenschutz-Aktivist und Journalist, verstärkte die Forderungen seiner Vorredenden, indem er verlangte: „Alle Staaten müssen die grundlegenden Menschenrechte respektieren!“ und „Leak more documents!“



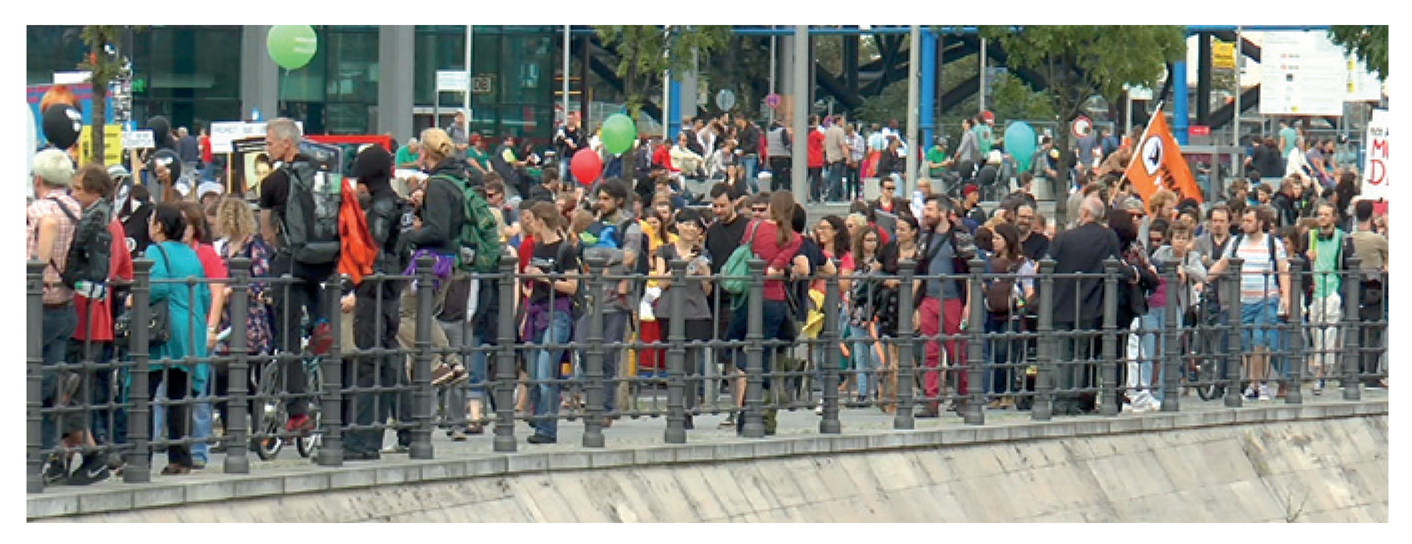


Christoph Bautz



„Massenüberwachung – das ist Gift für eine parlamentarische Demokratie und Honig für das Totalitäre“, stellte anschließend Christoph Bautz von Campact klar und richtete sich direkt an die Bundeskanzlerin: „Frau Merkel, bei diesem Skandal geht es nicht um Ihr Handy, bei diesem Skandal geht es auch nicht um einen Spion, bei diesem Skandal geht es darum, dass unser aller Handys überwacht, wir alle ausspioniert werden. Ihr Drumrumreden und Herunterspielen, Ihr Aussitzen und sich vor Konsequenzen drücken, das haben wir gewaltig satt!“ Hierfür gab es große Zustimmung – wie vorher bei der praktisch-parodistische „Rückensportübung für die Kanzlerin“. Für mehr Rückgrat in der Politik turnten die Demonstrierenden zusammen mit einer Kanzlerin-Darstellerin.

Anschließend zog der Demonstrationszug vom Brandenburger Tor / Straße des 17. Juni durchs Regierungsviertel über Ebertstraße, Dorotheenstraße und Wilhelmstraße bis durch die Luisenstraße, um später vorbei am Hauptbahnhof zum Kanzleramt zu kommen. Dort gab es eine Zwischenkundgebung, denn im Kanzleramt war „Tag der offenen Tür“, zu dem das Bündnis mit klaren Worten seinen aktiven Teil beigetragen hat.




Freiheit statt Angst




Wieland Dietrich

Bei der Abschlusskundgebung am Brandenburger Tor wurden konkrete Aspekte von Überwachungsbedrohungen aufgegriffen. So erklärte Wieland Dietrich, Vorsitzender der Freien Ärzteschaft e.V., zur elektronischen Gesundheitskarte: „Es wird offenbar, dass bei der elektronischen Gesundheitskarte der Druck der Gesundheitsindustrie auf die Politik enorm ist! Es ist ein Skandal, dass nach deutschem Recht überhaupt Daten, die dem Sozialdatenschutz unterliegen wie Gesundheitsdaten, von Rechenzentren verkauft werden dürfen!“ Auch Google mache mit diesen Daten Geschäfte. „Die elektronische Gesundheitskarte dient der Kontrolle der Bürger“, kritisierte Dietrich.


Astrid Goltz

Astrid Goltz von der Humanistischen Union nannte Fakten zu den Plänen der Bundesregierung für die Zukunft der Geheimdienste: „Im nächsten Jahr will die Bundesregierung den Etat des BND um 25 Prozent auf über 600 Mio. Euro erhöhen.“ Goltz kritisierte diesen Kurs scharf und forderte stattdessen die Abschaffung der Geheimdienste: „Merkel und de Maiziere machen keinen Finger krumm, um uns vor der massiven Überwachung unserer Privatsphäre zu schützen. Nein, sie päppeln ihre Geheimdienste mit Millionen an Steuergeldern auf und wir Bürger|innen bezahlen für unsere eigene Überwachung. Das ist absurd!“



Sebastian Schweda

„Die Enthüllungen der letzten Monate haben der ganzen Welt eine dramatische Erosion des Rechts auf Privatsphäre gezeigt“, warnte anschließend Sebastian Schweda von der Menschenrechtsorganisation Amnesty International. Er rief die Menschen zur Solidarität auf und stellte klar: „Das Spiel, das hier gespielt wird, heißt nicht USA versus Deutschland oder die ‘Five Eyes’ gegen den Rest der Welt. Das Spiel, das hier gespielt wird, heißt Regierung versus Bürger! Lassen Sie uns beim Thema Überwachung nicht vorzeitig aufgeben! Die Zeit ist mit uns!“

Um die Bürgerrechte von Sexarbeiterinnen und Sexarbeitern ging es in der Rede von Emy Fem vom Berufsverband erotische und sexuelle Dienstleistungen. Die geplante Zwangsregistrierung von in entsprechenden Berufen tätigen Menschen sei hochproblematisch „Sexarbeiter|innen werden entmündigt. Die Große Koalition geht davon aus, dass Sexarbeiter|innen nicht eigenverantwortlich handeln können, und zwar weil sie Sexarbeiter|innen sind.“ Eine Zwangsregistrierung bringe Gefahren für die Betroffenen, etwa durch Stalker oder gewalttätige Kunden.


Emy Fem


Matthias Spielkamp

Matthias Spielkamp von Reporter ohne Grenzen richtete seine Worte besonders an Menschen, die Informationen haben, die die ganze Gesellschaft betreffen: „Wer bei den Geheimdiensten, in anderen Behörden oder in Unternehmen arbeitet und sieht, dass dort gegen Gesetze verstoßen wird: Lasst es uns alle wissen!“

Nach den Beiträgen spielten verschiedene Bands zum Demo-Ausklang. An zahlreichen Ständen am Rande der Demo informierten viele beteiligte Organisationen über ihre spezifischen Themen.

Alle Reden sind auf YouTube abrufbar: https://www.youtube.com/playlist?list=PLKoKolf-IS-2NgC8QDlF8sr0Pyq-siDzD-

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

NSA-Partner CSC entwickelt Bundestrojaner

Aus einem vertraulichen BKA-Schreiben vom 10.02.2014 geht hervor, dass das Bundeskriminalamt (BKA) bei der Entwicklung von Überwachungssoftware eng mit der deutschen Tochter des umstrittenen US-Dienstleisters CSC zusammenarbeitet. In dem dreiseitigen Papier steht, dass CSC Deutschland „das BKA beim Projektmanagement und bei der Erstellung der Softwarearchitektur für die BKA-eigene Software zur Quellen-TKÜ“ unterstützt, also bei der Arbeit an einem sogenannten Bundestrojaner. Mit diesen Spähprogrammen soll die Kommunikation z. B. von Straftatverdächtigen über deren Computer abfangen werden. Das Verfassungsgericht hatte derartige Eingriffe 2008 verfassungsrechtlich bewertet und dadurch die bisherige Überwachungspraxis beendet. Seither arbeitet das BKA an einer neuen Lösung. Das Unternehmen CSC ist einer der wichtigsten IT-Dienstleister des US-Geheimdienstes NSA (Bundeskriminalamt lässt Überwachungssoftware mit US-Know-how entwickeln, Der Spiegel 29/2014, 12).

Bund

Versicherung von Cyber-Risiken

Versicherungsunternehmen haben entdeckt, dass mit der Absicherung von Internetschäden ein Geschäft gemacht werden kann. Bis zu 500 Milliarden Dollar verlieren Unternehmen laut einer Studie der Sicherheitsfirma McAfee aus dem Jahr 2013 durch den Verlust sensibler Daten. Neben der Wirtschaft haben auch Privatleute Angst, dass Cyber-Kriminelle ihre Kreditkartennummern missbrauchen oder sie bei Käufen im Netz übers Ohr hauen. Versicherer bieten spezielle Policen an, mit denen sich Verbraucher gegen solche Gefahren absichern können.

Der Düsseldorfer Rechtsschutzversicherer Arag, das einzige Versicherungsunternehmen Deutschlands in Familienbesitz, verspricht seit 2012 mit seiner Internet-Rechtsschutzpolice „Webaktiv“ umfassenden Online-Schutz. Die Police springt nicht nur bei Problemen mit Online-Käufen oder Kreditkartenbetrug ein, sondern auch, wenn der Kunde im Internet beleidigt wird oder der Nachwuchs die neuesten Computerspiele oder Kinofilme illegal aus dem Netz lädt. Sie richtet sich mit den Verträgen vor allem an Familien, so Arag-Vorstand Matthias Maslaton: „Eltern wissen relativ wenig darüber, was ihre Kinder im Internet so treiben“. Falls dann eine Abmahnung wegen eines illegalen Downloads ins Haus flattert, zahlt der Versicherer 190 Euro für eine Erstberatung beim Anwalt. Eventuelle Schadenersatzzahlungen müssen Kunden aber selber übernehmen. Auch die Kosten eines möglichen Verfahrens übernimmt der Versicherer nicht. Gemäß Maslaton kommt es aber meist gar nicht so weit, wenn Kunden sich mithilfe eines Anwalts wehren: „Das sind Massenverfahren. Die Firmen wollen sich gar nicht mit jedem Einzelnen auseinandersetzen. In 80 Prozent der Fälle klappt das.“

Auch bei Rufmord im Internet und in sozialen Netzwerken greift die Police. Kunden, die in Blogs, bei Facebook oder Twitter beleidigt werden, können sich an den Versicherer wenden. Dieser bezahlt einen Dienstleister, der versucht, die Beleidigungen aus dem Netz zu tilgen. Gemäß Maslaton klappt das in 80% der Fälle. Bei Prominenten sei das schwieriger, wie der Fall von Bettina Wulff zeigt. Die Frau des Ex-Bundespräsidenten setzt sich zur Wehr, dass ihr Name im Internet mit dem Rotlichtmilieu in Verbindung gebracht wird. Vom sogenannten Cyber-Mobbing sind vor allem Teenager betroffen. Es reicht von Beschimpfungen bis zur Verbreitung peinlicher Fotos oder Videos im Netz. Wenn Gespräche das Problem nicht aus der Welt schaffen, besorgt die Arag einen Mediator. Als letzter Ausweg bleiben rechtliche Schritte. Dafür bekommen die Kunden einen Anwalt bezahlt. Bis Mitte 2014 konnte das Unternehmen 14.700 Policen verkaufen. Diese kosten separat pro Jahr 113 Euro, als Zusatz zu einer Standard-Rechtsschutzpolice 79 Euro. Arag ist schon in 12 Ländern aktiv. 2014 werden Gesellschaften in Dänemark und Kanada gegründet.

Neben der Arag bietet auch der zum Kölner Rechtsschutzversicherer Roland gehörende Anbieter Jurpartner seit 2013 eine Internetpolice an, die bei Internetkäufen, Cyber-Mobbing oder Urheberrechtsverstößen einspringt. Auch bei einigen Rechtsschutzverträgen von Roland sind bestimmte Internetrisiken mitversichert. R+V kam mit einem eigenen Angebot 2014 auf den Markt und bietet darüber hinaus Schadenersatz, wenn Kunden auf betrügerische Online-Händler hereinfallen. Der Branchenriese Allianz überlegt, ebenfalls in den Markt mit Internet-Versicherungen einzusteigen. Die Münchner haben 2013 eine neue Police gegen Cyber-Risiken vorgestellt, mit der sich Unternehmen gegen die Folgen von Hacker-Angriffen oder Computerausfällen schützen können.

Die Verunsicherung vieler Verbraucher nach den Enthüllungen über das NSA-Ausspähprogramm hilft den Anbietern, so Arag-Vorstand Maslaton: „Immer wenn es solche Schlagzeilen gibt, erhöht das die Aufmerksamkeit.“ Einen umfassenden Schutz bietet bislang keine der Policen. Die Verträge von Arag und Jurpartner sind als Rechtsschutzversicherung konzipiert, das heißt, sie zahlen vor allem die Kosten für den Anwalt,

kommen aber nicht für einen eventuell entstandenen Schaden auf. Diesen Schutz bieten aber auch viele normale Rechtsschutzversicherungen. Verbraucherschützer halten deshalb nicht viel von den Policen. Timo Voss vom Bund der Versicherten: „Es handelt sich nur um eine Ausschnittsdeckung, und die ist eigentlich nicht sonderlich hilfreich. Anwaltliche Beratungen in solchen Fällen kosten in der Regel pauschal 400 bis 500 Euro plus Mehrwertsteuer.“ Die abgedeckten 190 Euro bei Urheberrechtsverletzungen genügten nicht. Auch der Schutz gegen Cyber-Mobbing und Shitstorms überzeugt den Verbraucherschützer nicht. Voss empfiehlt, sich den Deckungsumfang genau anzuschauen und gut zu überlegen, ob man die Police wirklich braucht. Denn nicht immer ist eine Spezialpolice nötig. Häufig sind Internetrisiken schon über altbekannte Versicherungen wie Haftpflicht- und Hausratversicherung abgedeckt. Verbreiten Computernutzer unwissentlich Viren, Trojaner oder Würmer und kommt es dadurch bei einem Dritten zu einem Schaden, springt die Haftpflichtversicherung ein. Laut dem Vergleichsportal Check24 decken 95% der aktuellen Haftpflichttarife diese Risiken mit ab.

Der Schutz bei Kreditkartenmissbrauch gehört laut Voss zum Standardumfang der meisten Rechtsschutzverträge. Phishing, also das Abgreifen sensibler Daten über vorgetäuschte E-Mails von Banken, ist häufig in Hausratpolicen mitversichert. Bei der Allianz sind etwa Phishing-Schäden beim Online-Banking inbegriffen. Ist viel Geld im Spiel, bleibt der Kunde aber auch hier auf einem Teil des Schadens sitzen. Der Versicherer zahlt je nach Vertrag zwischen 0,5% und 2% der Deckungssumme. Bei einer üblichen Deckungssumme von 65.000 Euro gibt es also maximal 1300 Euro (Policen gegen Cyber-Mobbing, SZ 12.06.2014, 20; Hagen, Schutz vor dem Shitstorm, www.sueddeutsche.de 28.07.2013).

Bund

„Quantified Self“ jetzt auch bei Krankenkassen

In den USA ist der Trend des „Quantified Self“, des „gezählten Ichs“ oder des „quantifizierten Selbst“ weit verbreitet. Aber auch immer mehr Deutsche entdecken ihre Freude am eigenen Körper als Datenquelle und werden dabei von Unternehmen sowie von Krankenkassen unterstützt beim Datenerfassen zu zurückgelegten Kilometern und Schritten, über Kalorienverbrauch pro Tag, Stresspegel, Stimmung, Alkohol- und Kaffeekonsum ... bis zur Schlafdauer und -tiefe. Gemessen, erfasst und ausgewertet werden die Daten zumeist über sog. smarte Armbänder und passende Apps für Fitness und Gesundheit.

Gemäß der Studie „Werte-Index 2014“ liegt Gesundheit bei deutschen Internetnutzern auf Platz eins der zentralen Werte, noch vor Freizeit und Erfolg. Trendforscher Peter Wippermann spricht sogar vom „Zeitalter der Selbstoptimierer“ und prophezeit, dass Gesundheit hierzulande zum wichtigen Branchenmotor wird, womit man auf Dauer Kosten einsparen, aber auch viel Geld verdienen kann. Krankenkassen haben den Trend aufgegriffen und bieten entsprechende Apps an. Damit kann der Kunde seine Körperdaten protokollieren und die Krankenkasse gesundheitsbewusstes Verhalten prämieren. Auf diese Weise wollen die Kassen vor allem bewegungsarme Patienten motivieren, um spätere Behandlungskosten zu sparen.

Die DAK bietet Mitgliedern die kostenlose FitCheck-App fürs Smartphone an. Bis Mai 2014 hatten sich 2.948 Kunden mit Versichertennummer und Gewicht registriert, um Bonuspunkte zu sammeln. Für 30 Minuten Radfahren, Skaten, Joggen oder 40 Minuten Walken gibt‘s je 50 Punkte, maximal 200 Punkte pro Monat und 2400 Punkte pro Jahr. Für die Punkte bekommt der Kunde später bis zu 150 Euro oder Prämien. Versicherte der Daimler-Betriebskrankenkasse, die gesund leben, zur Vorsorge gehen und Sport treiben, werden mit bis zu 100 Euro belohnt. Die sportlichen Anforderungen wie mindestens 100 Kilometer Laufen pro Jahr oder 250 Kilometer Radfahren lassen sich mit Sport-Apps wie Runtastic belegen.

Die AOK Nordost startete mit dem Schweizer Fitnessportal Dacadoo das Pilotprojekt AOK mobil vital. 730 Teilnehmer luden dazu die Dacadoo Tracker-App aufs Smartphone. Aus Geschlecht, Alter, Größe und Gewicht kalkulierte das Portal einen ersten „HealthScore“. Dieser Wert drückt sowohl Gesundheit als auch Fitness aus. Er liegt zwischen 1 (schlecht) und 1000 (hervorragend) und beruht auf klinischen Werten in der Dacadoo-Datenbank. Im Laufe des Projekts konnten die Teilnehmer den Wert verfeinern, indem sie regelmäßig sportliche Leistungen sowie Angaben zu Stimmung, Ernährung, Rauchen, Alkoholkonsum, Stresssituationen und Schlafphasen übertrugen. Derzeit wird die Pilotphase ausgewertet. Wenn sich der HealthScore der Teilnehmenden positiv entwickelt hat, soll der Wert in einem Prämienprogramm landen.

Andere Krankenversicherer halten sich mit Apps noch zurück und setzen stattdessen weiter auf die Mitgliedschaft in Vereinen oder den Besuch von Fitnesskursen. Denn die Möglichkeiten, mit Apps zu schummeln, sind groß: Wer kontrolliert schon, ob Sie selbst 30 Minuten gejoggt sind oder doch ein laufbegeisterter Freund? Träge Naturen fürchten, dass ihnen der Trend zur Selbstoptimierung Nachteile bringt. Carolin Wollschläger von der DAK-Pressestelle beteuert, dass Sammeln der Bonuspunkte durch sportliche Aktivitäten sei freiwillig, und „es ist nicht damit zu rechnen, dass dies einmal zur Pflicht wird“. AOK-Nordost-Pressesprecherin Gabriele Rähse beteuert, die Kasse erhalte bei der Auswertung des Pilotprojekts keine personenbezogenen Daten und somit keine Kenntnis, welcher Versicherte einen guten oder einen schlechten HealthScore hat.

Datenschützer sehen die Sammlung von Körperdaten kritisch. Marit Hansen, stellv. Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), fordert: „Wichtig ist, dass sich Verbraucher freiwillig für Selftracking entscheiden und das auch wieder ausschalten können. Leute, denen Privatsphäre wichtig ist, dürfen keine Nachteile haben.“ Diese Freiwilligkeit sieht der Hamburger Datenschützer Johannes Caspar gefährdet: „Sie wird zumindest dort infrage gestellt, wo Versicherungen durch die Überlassung der Gesundheitsdaten individuelle Risikoeinschätzungen vornehmen und besondere Tarife anbieten.“ Denn damit würden am Ende all jene belastet, die nicht in der Lage sind, positive Gesundheits-

daten online zu liefern oder dies ablehnen. Pharmaindustrie, Arbeitgeber, Versicherungen und Banken schielen ebenfalls auf die selbst erhobenen Daten. Damit können sie abschätzen, wie wahrscheinlich es ist, dass ein Mitarbeiter oder Kunde erkrankt. Es ist denkbar, dass Selbstvermesser ihnen künftig diese Daten für einen festgelegten Zeitraum gegen Bares überlassen. Ermöglichen soll das die Plattform Data Fairplay, die noch 2014 Verbraucher und Firmen gegen Provision zusammenbringen will. Datenschützer Caspar hat auch gegen Data Fairplay Bedenken: „Wollen wir in einer Gesellschaft leben, in der Menschen aus materieller Not ihre Daten an die meistbietenden Unternehmen verkaufen?“ (Brüggen-Freye, Kassen nutzen Fitness-Apps zur Datensammlung, www.welt.de 20.05.2014).

Bund

Krankenkassendaten teilweise unsicher

Die Patientendaten von mehreren Millionen gesetzlich versicherten Krankenkassenmitgliedern in Deutschland sind wenig geschützt. Mit einem Telefonanruf und wenigen Mausklicks könne jeder Unbefugte ohne technische Vorkenntnisse im Internet Details zu Arztbehandlungen, Diagnosen, verordneten Arzneimitteln, Krankenhausaufenthalten und andere intime Details abfragen. Das ist das Ergebnis eines Tests einer in Düsseldorf erscheinenden Zeitung am Beispiel der Barmer GEK. Die Barmer kündigte in einer Reaktion an, „die internen Kontroll- und Sicherheitsvorschriften erneut zu überprüfen und ggf. zu verschärfen“. Außerdem werde umgehend „ein weiteres Sicherheitsseminar für die Mitarbeiter durchgeführt.“ Auch das Bundesversicherungsamt kündigte als Aufsichtsbehörde Maßnahmen an: „Wir nehmen Ihre Schilderungen zum Anlass, die Rechtssicherheit der Kommunikation zwischen Versicherten und Krankenkassen einer grundsätzlichen Prüfung zu unterziehen.“ Bei dem Test genügten der Zeitung nach der Name eines beliebigen Versicherten, sein Geburtsdatum und seine Versichertennummer. Allein mit diesen Informationen war der Zugriff auf hochsensible Patientendaten möglich. Auch bei anderen Krankenversicherungen wie AOK, Techniker, DAK oder Betriebskrankenkassen gibt es die Möglichkeit, die Daten im Internet zu verwalten. Allerdings wurden diese nicht getestet (Patientendaten sind unsicher, www.wiwo.de 26.06.2014).

Bund

Bundestag verkürzt eigene Vorratsdatenspeicherung

Gemäß einer Vorlage des Ältestenrates des Deutschen Bundestags soll die interne Datenspeicherpraxis des Parlaments dahingehend verändert werden, dass die Verbindungsdaten von Abgeordneten und ihren Mitarbeitenden statt bisher drei Monate künftig nur noch sieben Tage gespeichert werden. Die Obleute der sogenannten IuK-Kommission einigten sich auf diese Änderung. Zudem sollen die Parlamentarier mehr Mitsprache dabei bekommen, wie lange Sicherheitskopien ihrer E-Mails und Dateien aufbewahrt werden. Erst kurz zuvor war bekannt geworden, dass der Bundestag sämtliche Kommunikationsdaten der Abgeordneten rund drei Monate lang speichert. Die Regelungen stammen aus dem Jahr 2008. In den Fokus rückte die Speicherpraxis im Zuge der Affäre um Sebastian Edathy.

Die Bundestagsverwaltung speichert neben den Verbindungsdaten auch die vollständigen Adressen der besuchten Seiten sowie Größe und Name von heruntergeladenen Dateien und die E-Mail-Adressen von Sendenden und Empfängern. Die Neuregelung soll die Abgeordneten auch für den Umgang mit den eigenen Daten sensibilisieren. Die künftige siebentägige Speicherfrist für Protokolldaten soll künftig nur „im begründeten Ausnahmefall“ und „mit Einverständnis der Vorsitzenden der IuK-Kommission erhöht werden“ können. Die Parlamentarier sollen künftig über die Einrichtung eines Sicherheits-Backups selbst entscheiden: „Die Datensicherung von E-Mails und Dateien soll so individualisiert werden, dass jedem Abgeordneten die Möglichkeit gegeben werden kann, in eigener Verantwortung zu entscheiden, ob und über welchen Zeitraum seine Daten gesichert werden sollen.“ Steffi Lemke, grüne Obfrau in der IuK-Kommission, begrüßte die Verkürzung der Speicherfristen und die Individualisierung der Datensicherung: „Insgesamt haben wir aber bei der Sensibilisierung für Datenschutzbelange auch als Parlament noch einiges aufzuholen“ (Medick/Meiritz, Bundestag will Daten nur noch sieben Tage speichern, www.spiegel.de 05.06.2014).

Bund

Monopolkommission hat Datenschutz „entdeckt“

Die Monopolkommission, ein fünfköpfiges beratendes Expertengremium der deutschen Bundesregierung, forderte Anfang Juli 2014 in ihrem alle zwei Jahre erscheinenden Hauptgutachten, über eine „verstärkte Kooperation“ von Datenschutz- und Wettbewerbsbehörden nachzudenken. Es sei an der Zeit zu hinterfragen, „ob die bestehenden Wettbewerbsregeln für die Bewältigung derartiger Probleme überhaupt geeignet sind“. Gemeint ist damit u. a., dass das Kartellamt in Konflikten zwischen Internetdienstleistern und Inhaltsanbietern vorrangig „zum Nachteil“ Letzterer entscheidet und das Problem des Zugriffs auf Nutzerdaten „nur sehr mittelbar“ adressiert. Die bestehende Rechtslage erlaube es nicht anders, man habe es schlicht mit „häufig noch nicht erforschten Marktkräften im Internet“ zu tun. Die rechtliche Stellung der Monopolkommission ist gesetzlich nicht geregelt. Die Aufgaben der Monopolkommission ergeben sich aus § 44 bis § 47 Gesetz gegen Wettbewerbsbeschränkungen (GWB).

Im April 2014 hatte Wirtschaftsminister Sigmar Gabriel der Monopolkommission noch vorgeworfen, sich um die Internetgiganten nicht zu scheren und stattdessen Regionalmonopole, etwa von Sparkassen, zu hinterfragen. Im Mai 2014 verwahrte sich Kartellamtschef Andreas Mundt dagegen, für Datenschutz zuständig zu sein. Nun meint die Monopolkommission, die „Funktionsfähigkeit datenbasierter Geschäftsmodelle“ könne gar nicht allein wettbe-

werbsrechtlich betrachtet werden, da die Nützlichkeit eines Internetdienstes von der detaillierten Beobachtung des Verhaltens der Nutzer abhänge. Das Sammeln personenbezogener Profil- und Verhaltensdaten gehöre ins Zentrum des Wettbewerbsrechts: „So bietet beispielsweise Google seinen Nutzern neben der Internetsuche eine Fülle weiterer oft unentgeltlicher Dienstleistungen und Produkte an, die es dem Unternehmen erlauben, mehr Daten über seine Nutzer zu sammeln.“ Dieses datenschutzrechtlich kritisierte Phänomen mache aus dem Wettbewerb auf dem Markt einen „Wettbewerb um den Markt“. Die Netzwerkeffekte und Synergien, die Google und andere Anbieter nutzen, die wie „Hebeleffekte“ die „Übertragung der Marktposition von einem beherrschten Markt auf andere Märkte“ ermöglichen, seien bisher unverstanden.

Die Monopolkommission verneint die Fragen, ob Suchanbieter monopolträchtig sind und die Gefahr natürlicher Monopole prinzipiell in digitalen Märkten schlummere: Ein Suchanbieter sei keine „wesentliche Einrichtung“. Diese Kategorie gelte grundsätzlich nur für wenige „physische Infrastrukturen“ wie Brücken, die sich von Konkurrenten nicht wahllos duplizieren ließen. Das Recht wie auch die dahinter stehenden analogen Denkmodelle seien für die Beobachtung der digitalen Ökonomie unbrauchbar. Google vereine rund 90% aller deutschsprachigen Suchanfragen im Internet auf sich. Aber schon der Markt für Internetsuchen sei vom Markt für die Buchung von Werbeplätzen in Suchergebnissen zu unterscheiden. Nach deutschem Recht handele es sich nicht um zwei Seiten desselben Marktes, auf dem die Aufmerksamkeit von Nutzenden an Werbetreibende verkauft werde. Es gebe stattdessen allenfalls beobachtbare „Interdependenzen“. Die tatsächlichen Grenzen der Märkte seien „kartellrechtlich nur schwer abzubilden“. Die Behörden hätten daher keine Wahl, als in Konfliktfällen die Zusagen von Unternehmen als wichtiges Mittel anzusehen, von Bestrafungen abzusehen und zu hoffen, dass die Kraft innovativer Unternehmen stärker sei als die der etablierten Unternehmen im Versuch, ihre Märkte abzuschotten. Das Risiko „einer wettbewerbsfeindlichen Ausnutzung von Marktpositionen zur Abschottung von Märkten“ bestehe trotz allen Unvermögens, der Probleme rechtlich Herr zu werden. Die mangelhafte Gesetzeslage „schließt es freilich nicht aus“, dass Dienste „eine hohe wirtschaftliche Bedeutung haben können“, aus der sich eine „besondere Verantwortung“ ableiten lasse. Die Behauptung, ein Konkurrent sei „nur einen Mausklick entfernt“, stimme häufig nicht. Für Suchmaschinenanbieter gelte das ebenso wie für Anbieter sozialer Netzwerke.

Die Kommission unterstreicht die Überlegungen von Sigmar Gabriel, dass das wettbewerbsrechtliche Instrumentarium für den Schutz der Verbraucher „nicht ungeeignet“ wäre. Der von ihm angedrohte mögliche letzte Ausweg, große Anbieter von Internetdiensten zu entflechten, sei jedoch eine „drastische Maßnahme“, die das Wettbewerbsrecht überfordern könnte. Diese Diskussion solle versachlicht werden, um zu ermitteln, welche rechtlichen Mittel angezeigt und gerechtfertigt wären. Mit dem Urteil des Europäischen Gerichtshofs (EuGH) gegen Google vom 13.05.2014 gäbe es eine erste Grundlagenentscheidung, nach der europäisches Datenschutzrecht in Europa auch für außerhalb Europas ansässige Internetdienstanbieter anwendbar sei. Dasselbe Prinzip gelte nun auch für deutsches Wettbewerbsrecht in Auseinandersetzungen zwischen hiesigen und beispielsweise amerikanischen Unternehmen. Ähnlich wie der EuGH unterstreicht die Monopolkommission die rechtliche Einordnung der Anbieter „universeller Internetsuchen“. Anders als Medienhäuser, Verlage und Internetdienstleister mit thematischen Angeboten hätten Unternehmen wie Google, Bing und Yahoo, die eine „horizontale Suche“ anböten, auch im Wettbewerbsrecht eine herausgehobene Stellung. Ihr Markt lasse sich nämlich nicht eindeutig abgrenzen. Es wäre jedoch verkürzt, hierbei allein mit dem Wettbewerbsrecht zu reagieren. Eine Entflechtung würde übersehen, von welcher gesellschaftlichen Bedeutung die Dienste inzwischen sein können. Stattdessen setzt die Monopolkommission auf Hilfe aus dem Datenschutzrecht. Die derzeit verhandelte europäische Datenschutz-Grundverordnung (EU-DSGVO), die bisher von der Bundesregierung politisch gebremst wurde und wird und die zugleich z. B. von Wirtschaftsminister Gabriel als „scharfes Schwert“ gepriesen wird, ist nach Ansicht der Monopolkommission auch für das Wettbewerbsrecht von „besonderer Bedeutung“. Die Regeln würden „Nutzern ermöglichen, selbstbestimmt über ihre Daten zu entscheiden und den Dienstanbietern auf Augenhöhe entgegenzutreten“.

In der Praxis tun sich die Kartellbehörden noch schwer: So prüft z. B. die EU-Wettbewerbsbehörde den Kauf des Kurznachrichtendienstes WhatsApp durch Facebook für 19 Mrd. Euro, nachdem in drei EU-Mitgliedstaaten – Großbritannien, Spanien und Zypern – die nationalen Behörden aus jeweils anderen Wettbewerbsgründen eine Kontrolle durchführen, was der EU die Möglichkeit eröffnet hat, das Verfahren an sich zu ziehen. In Deutschland konnte das Bundeskartellamt nicht aktiv werden, weil der nationale Umsatz von WhatsApp unter 5 Mio. Euro liegt, obwohl über 30 Mio. Deutsche den Dienst nutzen. Der wahre Wert von WhatsApp lässt sich nicht mit Umsatzzahlen messen. So will Facebook mit dem Kauf an die Nutzerdaten aus 10 Mrd. Nachrichten, 700 Mio. Fotos und 100 Mio. Videos herankommen, die weltweit jeden Tag über WhatsApp verschickt werden. Die EU-Behörde hat nun Konkurrenten der beiden Firmen angeschrieben, um mehr über die Wettbewerbswirkung der im Februar 2014 von Facebook-Gründer Mark Zuckerberg angekündigten Übernahme zu erfahren. WhatsApp will mithilfe von Facebook z. B. kostenlose Telefonate anbieten. Auch soll untersucht werden, wie Facebook die Daten der mehr als 500 Mio. WhatsApp-Nutzenden verwerten will (Der Spiegel 29/2014, 64; Schulz, Schützt unsere Daten besser, www.faz.net 11.07.2014 = FAZ 12.07.2014, 17).

Bundesländer

Taschenrechner-Verkäufer sammeln SchülerInnendaten

Bundesweit tätige Anbieter von Schultaschenrechnern animierten Lehrkräfte offenbar systematisch zu Ver-

stößen gegen das Schul- und Datenschutzrecht. Behörden in mehreren Bundesländern prüfen deswegen die bei Klassen-Sammelbestellungen angewandten Verfahren. In Niedersachsen hat die Landesschulbehörde ein erstes Ordnungswidrigkeitsverfahren gegen einen Lehrer eingeleitet. Er hatte an dem Bestellverfahren teilgenommen und Daten seiner Schüler an einen Händler weitergegeben.

Konkret geht es um sog. CAS-Taschenrechner, die aufwendige Graphen anzeigen und ganze Gleichungssysteme mit Unbekannten lösen können. In den meisten Bundesländern kommen diese Geräte bereits ab der siebten Klasse zum Einsatz. Im Handel können die Rechner bis zu 150 Euro kosten. Darauf spezialisierte Online-Anbieter verkaufen sie bei Sammelbestellungen von Schulen schon für etwa 115 Euro. Die Abwicklung übernimmt dabei in der Regel die Lehrkraft. Und so wirbt der Betreiber der Internetplattform Taschenrechner.de auf seiner Seite: „Nie wieder Listen anlegen und Zahlungseingänge kontrollieren! Testen Sie unsere Bequemzahlung: Einfacher geht es nicht!“ Die attraktive Botschaft für die PädagogInnen: Ärgern Sie sich nicht mit den Formalitäten herum, das erledigen wir! Der Händler benötigt aber eine „alphabetisch sortierte Namensliste aller(!) Schüler der betreffenden Jahrgangsstufe klassenweise in einer Exceldatei“ – und das unabhängig von der Frage, welche Schüler bei der Sammelbestellung überhaupt mitmachen.

Der Vorsitzende des schleswig-holsteinischen Philologenverbandes, Helmut Siegmon, selber Mathelehrer, sieht dieses vermeintlich angenehme Bestellverfahren kritisch: „Ich halte es für unseriös, das ist natürlich nicht in Ordnung.“ Gleich zwei Rechtsverstöße hält Schleswig-Holsteins Datenschutzbeauftragter Thilo Weichert für möglich: „Nach unseren Erkenntnissen werden hier ganz offensichtlich die Lehrer animiert, Daten von SchülerInnen für Werbezwecke weiterzugeben – das ist nach dem Datenschutzrecht und nach dem Schulgesetz definitiv nicht erlaubt.“ Notwendig wäre, vor der Übermittlung eine explizite, schriftliche Einwilligung jedes Schülers zur Datenübermittlung einzuholen. Seine Behörde prüft, welche Sanktionsmöglichkeiten in Frage kommen.

Betreiber der Internetseite Taschenrechner.de ist die Böttcher Datentechnik GmbH mit Sitz in Lübeck. Deren Geschäftsführer, Detlef Böttcher, erklärte, ein Datenschützer habe vor einiger Zeit dieses Verfahren geprüft. Er räumte allerdings ein, dass sein Unternehmen nicht überprüft, ob die Lehrer vor der Übermittlung der Schülerlisten an sein Unternehmen die Einwilligungen von Schülern oder Eltern eingeholt haben. „Es ist nicht unsere Aufgabe, zu kontrollieren, ob eine Einverständniserklärung vorliegt.“

Die Landesschulbehörde in Niedersachsen ist schon einen Schritt weiter als die Datenschützer in Kiel. Sie hat ein Ordnungswidrigkeitsverfahren gegen einen Lehrer eingeleitet. Er hatte in der Vergangenheit das Bequemzahlungsverfahren des Lübecker Händlers genutzt. Das Niedersächsische Kultusministerium arbeitet deswegen momentan an einer neuen Richtlinie für vergleichbare Bestellungen.

Ebenfalls Ärger bekommen könnte ein weiterer bundesweit tätiger Schultaschenrechner-Händler aus Thüringen. Er bietet auf seiner Online-Plattform ein vergleichbares Sammelbestellungsverfahren an, für das sich inzwischen der dortige Landesbeauftragte für Datenschutz interessiert. Je nachdem wie dort das Bestellverfahren durchgeführt wird, hält die Behörde einen „schweren datenschutzrechtlichen Verstoß“ für möglich. Auch dieser Anbieter meinte, er tue alles dafür, dass die gesetzlichen Vorgaben eingehalten würden (Meyer/Mügge, Taschenrechner-Händler sammeln Schüler-Daten, www.ndr.de 21.05.2014).

Bundesländer

Straßenansichtserfassung durch Nokia

Nach Google (Google Streetview) und Microsoft (Bing Maps Streetside) fährt auch die Firma Nokia mit Kamerafahrzeugen u.a. durch Baden-Württemberg, Bayern und Berlin und nimmt Straßenansichten auf. Die Nokia Corporation, ein in Finnland ansässiges Unternehmen, tut dies mit Autos der niederländischen Tochtergesellschaft „HERE Europe B. V. („Here“)“. Dabei sollen nach Angaben von Nokia bereits bestehende digitale Straßenkarten, die unter anderem in Navigationsgeräten Verwendung finden, qualitativ verbessert werden. Vor einer ebenfalls vorgesehenen Veröffentlichung der Aufnahmen im Internet sollen die Aufnahmen gemäß dem Unternehmen so bearbeitet werden, dass darauf zu findende, zufällig aufgenommene Personen oder Kraftfahrzeugkennzeichen unkenntlich gemacht werden. Das bearbeitete Bildmaterial soll frühestens sechs Monate nach der Erhebung der Daten veröffentlicht werden.

Die Aufnahmen werden in einzelnen Städten und Regionen mit Hilfe von auf PKW installierten Kameras durchgeführt. Die PKW sind entsprechend mit dem HERE Logo gekennzeichnet. Wo die PKW fahren, kann man dem folgenden Link entnehmen: http://here.com/legal/driveschedule. Ebenso werden nach Angabe von Nokia die Zeitpunkte der Kamerafahrten, soweit technisch möglich, in aktualisierter Form unter dem genannten Link bekannt gegeben. Darüber hinaus bietet das Unternehmen betroffenen BürgerInnen, die einer Veröffentlichung ihrer Hausfassade widersprechen oder sonstige Fragen und Beschwerden vortragen möchten, eine direkte Kontaktaufnahme in deutscher Sprache per E-Mail unter privacy@here.com oder per Briefpost, die an die Nokia Corporation, c/o Privacy, Karakaari 7, 02610, Espoo, Finnland, zu richten ist, an. Der berliner Datenschutzbeauftragte Alexander Dix erklärte: „Ich empfehle allen Bürgerinnen und Bürgern, die nicht mit der Veröffentlichung ihrer Hausfassade im Internet einverstanden sind, sich direkt an das Unternehmen zu wenden und der Veröffentlichung zu widersprechen.“ Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bietet den BürgerInnen an, bei Problemfällen zu helfen, wenngleich wegen des Sitzes der Firma Nokia in Finnland das finnische Datenschutzrecht anwendbar sei (BayLDA, Nokia erfasst Straßenansichten in Bayern, PE 10.06.2014; LfD Baden-Württemberg, Baden-Württembergische Städte werden von Nokia abfotografiert, PE 27.06.2014; BlnBDI PM 25.06.2014, Nokia erfasst Straßenansichten in Berlin).

Bayern

Drohne filmt Nackte

In Landshut hat sich ein 62-jähriger Spanner mit einem ungewöhnlichen Mittel auf die Jagd nach unbekleideten Opfern gemacht: Der 62-Jährige filmte mit einer Drohne in einen ansonsten uneinsehbaren Garten, in dem sich eine 47 Jahre alte Frau und ihr Freund nackt sonnten. Der fernsteuerbare Mini-Hubschrauber fiel am 24.07.2014 auf, weil er längere Zeit über einer Garage in der Luft stand. Wie die Polizei am Tag darauf berichtete, wurde gegen den Drohnen-Piloten gemäß § 201a Strafgesetzbuch „wegen Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen“ ein Strafverfahren eingeleitet (Spanner filmt Nackte mit Drohne, SZ 26./27.07.2014, 10).

Thüringen

Staatsanwalt: journalistische Kamerabrille zulässig

Die Staatsanwaltschaft Erfurt hat die Ermittlungen gegen eine Journalistin wegen verdeckter Recherchen beim Online-Modehändler Zalando eingestellt. Staatsanwaltssprecher Hannes Grüneisen erklärte am 09.07.2014: „Es liegt kein strafbares Verhalten vor.“ Die journalistische Tätigkeit mit einer Kamerabrille für das Rechercheteam Günter Wallraff sei nicht strafbar. Der Verdacht auf Verrat von Geschäfts- und Betriebsgeheimnissen habe sich nicht bestätigt. Die RTL-Reporterin hatte drei Monate lang im Erfurter Zalando-Logistikzentrum gearbeitet. Sie hatte dem Unternehmen in der Sendung „Extra“ vorgeworfen, Angestellte massiv unter Druck gesetzt und gegen das Arbeitsrecht verstoßen zu haben (Ermittlungen nach verdeckter Recherche bei Zalando eingestellt, www.focus.de 09.07.2014).

Datenschutznachrichten aus dem Ausland

Weltweit

Axa-Versicherungskonzern setzt auf Digitalisierung

Der Chef des Axa-Versicherungskonzerns Henri de Castries hat vor JournalistInnen im Juni 2014 in Suduiraut bei Bordeaux/Frankreich seine Konzernstrategie in der globalisierten Informationsgesellschaft dargelegt. Axa gehört mit 91 Mrd. Euro Jahresumsatz zu den Weltmarktführern und liegt auf Augenhöhe mit der Allianz, die 2013 auf 111 Mrd. kam. Er legte zwei Trends dar: In der globalen Wirtschaft würden sich die Gewichte verändern – weg von den gesättigten Märkten Europas, Nordamerikas und Japans, hin zu den Schwellenländern. Dieses „Problem“ lasse sich mit Milliardeninvestitionen, Zukäufen und Neugründungen in den Schwellenländern lösen. Axa engagierte sich jüngst in China und Kolumbien; die brasilianische Bank Itáu Unibanco steht auf der Wunschliste, für die sich aber auch die deutsche Talanx-Gruppe interessiert.

Das zweite „Problem“ sieht de Castries in der digitalen Revolution, welche die Branche umkrempele. Wer viel über die KundInnen weiß, könne zielgenaue Angebote machen. Die Daten kämen aus den sozialen Netzwerken, aus den Black Boxes von Autos, aus den Gesundheits-Apps mit Armbändern von Apple und Google und aus den Rechenzentren der Versicherer selbst, die bisher keine Ahnung hätten, was sie über ihre KundInnen heute schon alles wissen. Wenn die Versicherer die Informationen nicht nutzen, gerieten sie ins Hintertreffen. Datenriesen wie Google, Facebook oder Amazon drängten früher oder später in das Geschäftsfeld. Ein Jahr zuvor hatte Castries deshalb noch auf die drei Internet-Unternehmen geschimpft und Waffengleichheit verlangt. Jetzt sucht er den Schulterschluss und kann sich selbst den Verkauf von Policen über den Online-Händler Amazon vorstellen: „Wenn das für die Kunden interessant ist, warum nicht?“

Axa hat inzwischen im Silicon Valley ein Labor mit fünf Experten gegründet, die als Technik-Scouts neue Entwicklungen aufspüren und den Kontakt zu den Online-Anbietern halten sollen. Mit Facebook wurde ein Kooperationsvertrag geschlossen, was Véronique Weill, Chief Operating Officer, erläutert: „Dabei geht es vor allem um die Ausbildung unserer Mitarbeiter.“ Herauskommen soll eine enge Verbindung von Vertrieb und Kundenbetreuung über PC, Tablet und vor allem Smartphone mit den bestehenden Vertretern und Maklern. Von 2013 bis 2015 gibt der Konzern für die Digitalisierung 800 Mio. Euro aus – budgetiert waren zunächst nur 600 Millionen.

Castries und Weill betonten, der Datenschutz spiele eine zentrale Rolle. Der sei aber von Land zu Land sehr verschieden ausgeprägt: „Den Amerikanern ist das egal. Die Deutschen sind hypersensibel an dieser Stelle, mehr als in jedem anderen Land.“ Die Franzosen stünden da in der Mitte. „Wir müssen das respektieren. Wir respektieren ja auch die verschiedenen Gesetze in den Ländern.“ Wer nicht wolle, dass seine Daten genutzt werden, habe deshalb keine Probleme. „Nur, wer uns Daten gibt, kann damit Geld sparen“ (Fromme, Suche nach der Datenhoheit, SZ 10.06.2014, 26).

UNO

Menschenrechtskommissarin: Aufruf gegen Massenüberwachung

Die UN-Hochkommissarin für Menschenrechte, Navi Pillay, stellte am 16.07.2014 in Genf einen Bericht zur

Internetüberwachung des privaten Datenverkehrs vor, die höchst besorgniserregende Ausmaße angenommen habe: Massen-Überwachungen durch Regierungen „entwickeln sich zu einer gefährlichen Gewohnheit und sind keine Ausnahme mehr". Die Praktiken in vielen Staaten zeigten Mängel bei einer angemessenen nationalen Gesetzgebung und einer entsprechenden Strafverfolgung. Auch deswegen ermutigt die Kommissarin Pillay Firmen, die von Regierungen zur Weitergabe von Daten gedrängt würden, sich stärker zu wehren. Die National Security Agency (NSA/USA) und der britische Government Communications Headquarters (GCHQ), aber auch andere westliche Geheimdienste greifen in großem Umfang internationale Kommunikation ab, spionieren Unternehmen sowie staatliche Stellen aus und verpflichten Dienstleister im Geheimen zur Kooperation, wie ursprünglich streng geheime Dokumente zeigen, die der Whistleblower und ehemalige NSA-Analyst Edward Snowden an sich gebracht und an Medien weitergegeben hat.

Laut Pillay sind Programme zur massenhaften Überwachung von E-Mails selbst dann zu hinterfragen, wenn sie legitime Ziele hätten. Es reiche nicht aus, wenn gezielt die Nadel im Heuhaufen gesucht werde: „Der angemessene Maßstab ist die Wirkung auf den Heuhaufen im Vergleich zur Bedrohung." Als eine Maßnahme empfiehlt Pillay die Einrichtung unabhängiger Institutionen, die die Überwachung unter die Lupe nehmen. „Einige unglaublich wichtige Prinzipien, die den Kern jedermanns Persönlichkeitsrechte betreffen, stehen auf dem Spiel." Die UN-Hochkommissarin wies darauf hin, dass Firmen, die den Regierungen Daten zur Verfügung stellten, selbst riskierten, zum Mittäter bei Menschenrechtsverletzungen zu werden. Falls es solche Regierungsanfragen gebe, sollten Unternehmen so knapp wie möglich darauf eingehen, die rechtliche Begründung klären und gegebenenfalls erst auf Drängen eines Gerichts kooperieren. „Es gibt dafür positive Beispiele in der Industrie, sowohl von einzelnen Firmen als auch von Bündnissen von Unternehmen und Interessensgruppen." Der Bericht ist auf Wunsch der Vollversammlung der Vereinten Nationen erstellt werden. Im Dezember 2013 war eine von Deutschland und Brasilien eingebrachte Resolution gegen Internetspionage angenommen worden. Darin war die Hochkommissarin für Menschenrechte aufgefordert worden, sich mit dem „Schutz der Privatsphäre bei digitaler Kommunikation" zu befassen. Der Bericht soll im Oktober in der UN-Vollversammlung vorgestellt und beraten werden (UN: Firmen sollen sich gegen zunehmende E-Mail-Überwachung wehren, www.heise.de 16.07.2014).

Großbritannien

Geheimdienstaktivitäten vor Gericht

In Großbritannien müssen sich die eigenen Geheimdienste, insbesondere das Government Communications Headquarters (GCHQ), seit dem 14.07.2014 vor Gericht gegen den Vorwurf von zehn britischen und ausländischen Bürgerrechtsgruppen wehren, die vom Ex-US-Geheimdienstmitarbeiter Edward Snowden enthüllte Massenüberwachung verstoße gegen Menschenrechte. Vor dem im Jahr 2000 geschaffenen Geheimdiensttribunal begann eine Serie von Anhörungen, die die Bürgerrechtsorganisationen als historisch werteten. Eine Regierungssprecherin lehnte zunächst eine Stellungnahme zu den konkreten Fällen ab. Sie betonte aber, die britischen Ausspäh-Regeln stünden in Einklang mit der Europäischen Menschenrechtskonvention. Weil die verantwortlichen Minister die Existenz von Programmen wie Tempora und Prism weder dementieren noch bestätigen, finden die Anhörungen auf Grundlage „vereinbarter hypothetischer Fakten" statt. Es wird so getan, als träfen die durch Snowden veröffentlichten Informationen zu (SZ 15.07.2014, 8).

Großbritannien

GCHQ verfälscht Daten im Netz

Der britische Geheimdienste Government Communication Headquarters (GCHQ) erklärt gemäß Dokumenten des Whistleblowers Edward Snowden,



Online-Umfragen manipulieren, den Traffic auf Internetseiten verfälschen oder nicht genehme Videos zensieren zu können. Das berichtet Glenn Greenwald auf The Intercept. Auf einer online gestellten Liste finden sich verschiedenste Werkzeuge und eine kurze Beschreibung ihrer Fähigkeiten.

Die Fähigkeiten des GCHQ richten sich demnach nicht nur gegen Daten oder Inhalte im Netz, sondern auch gegen Dienste möglicher Zielpersonen. So können etwa zwei Telefone miteinander in einem Gespräch verbunden werden (Imperial Barge). Die Möglichkeit, E-Mails zu senden oder zu empfangen kann ebenso unterbunden werden, wie die Möglichkeit Inhalte im Netz anzusehen (Sunblock). Zur Unterstützung einer „Informationskampagne" können demnach auch massenhaft SMS und E-Mails versendet werden. Die Kommunikation auf Skype kann überwacht werden (Miniature Hero). Die aufgeführten Tools und Fähigkeiten des GCHQ sind angesichts der seit Monaten anhaltenden Enthüllungen über die Aktivitäten westlicher Geheimdienste nicht überraschend und waren teilweise in Dokumenten bereits erwähnt worden. Die Liste unterstreicht jedoch eindringlich, dass der britische Geheimdienst offensichtlich auch tut, wozu er technisch in der Lage ist. So heißt es in dem GCHQ-Dokument: Wenn etwas nicht in der Liste stehe, bedeute das nicht, „dass wir es nicht bauen können". Die neue Enthüllung kommt zu einem Zeitpunkt, zu dem in

Großbritannien gerade im Eilverfahren ein neues Überwachungsgesetz durch das Parlament gebracht wird. Damit soll im Prinzip die vom EuGH gekippte Vorratsdatenspeicherung und damit ein Teil der umfangreichen Überwachung beibehalten werde (NSA-Skandal: GCHQ verfälscht Daten im Netz, www.heise.de 15.07.2014).

Norwegen

Geheimdienstkooperation mit NSA und Supercomputer

Der norwegische Militärgeheimdienst Etteretningstjenesten (Etjenesten) kauft im Rahmen einer Budgetsteigerung von 600 Mio. Norwegischen Kronen (ca. 70 Millionen Euro) einen Supercomputer, um täglich gesammelte gewaltige Telekommunikations-Datenmengen zu verarbeiten. Gemäß Zeitungsberichten, die auf Dokumente des NSA-Whistleblowers Edward Snowden zurückgehen, hat der norwegische Geheimdienst mit der NSA vereinbart, gemeinsam Anwendungen für die immense Rechenkapazität von Steelwinter, einem Derivat eines IBM-Supercomputers namens Windsor Blue zu entwickeln. Der Kauf sei im März 2013 zwischen den beiden Geheimdiensten aus Norwegen und den USA besprochen worden. Wann der Supercomputer geliefert werden soll, ist unklar. Gleichzeitig sei eine Zusammenarbeit bei Versuchen zur Entschlüsselung abgegriffener Inhalte vereinbart worden. Dabei solle der Computer genauso helfen wie bei der Suche nach den „Nadeln in den Heuhaufen" der massenhaft abgegriffenen Kommunikationsdaten. Bislang seien die Daten häufig in die USA zur NSA geschickt worden; nun soll dies vor Ort in Norwegen geschehen.

Schon zuvor war bekannt geworden, dass der norwegische Geheimdienst allein im Dezember 2013 insgesamt 33 Millionen Telefongespräche abgegriffen hat. Entgegen ursprünglicher Berichte handelte es sich dabei aber offenbar nicht um norwegische Telefonate, sondern um welche in Afghanistan. Außerdem werde von einer Station in Vardø – nahe der Grenze zu Russland – Satelliten- und Radiokommunikation mitgeschnitten. Auch für die dabei anfallenden gewaltigen Datenmengen werde der Supercomputer angeschafft (NSA-Skandal: Norwegens Geheimdienst kauft Supercomputer, www.heise.de 27.04.2014).

Kanada

Links auf rechtsverletzende Websites sind zu löschen

Der Supreme Court der kanadischen Provinz British Columbia hat Google mit Urteil vom 13.06.2014 dazu verdonnert, Links auf rechtsverletzende Webseiten global aus dem eigenen Suchindex zu entfernen. Ein Unterdrücken der Treffer auf dem kanadischen Google-Portal reicht demnach nicht aus, um künftige weitere Rechtsverstöße zu verhindern. Echte Abhilfe schaffe nur eine Blockade der inkriminierten Angebote in der globalen Datenbank der Kalifornier.

Die Entscheidung baut teilweise auf dem Urteil des Europäischen Gerichtshofs (EuGH) vom 13.05.2014 auf, wonach Google dazu verpflichtet werden kann, Verweise auf Webseiten mit sensiblen persönlichen Daten aus seiner Ergebnisliste zu streichen. Geklagt hatte in dem kanadischen Fall die Firma Equustek Solutions, die unter anderem komplexe Netzwerkgeräte für die Industrie herstellt. Der Kläger warf früheren, jetzt unter dem Dach des Unternehmens DataLink Technologies Gateways agierenden Mitarbeitern vor, Geschäftsgeheimnisse gestohlen und Geräte nachgebaut zu haben.

Der Supreme Court erkennt analog zum EuGH an, dass Google auch mit der Tätigkeit aus Kalifornien heraus Kanadier anspricht und so kanadischem Recht unterliegt. Dass Google letztlich auch der Rechtsprechung jedes Nationalstaats weltweit unterliege, sei eine natürliche Folge des globalen Geschäftsmodells der Kalifornier, so die Vorsitzende Richterin Lauri Ann Fenlon. Google sei zwar ein „unbeteiligter Zuschauer" in dem Verfahren. Der Internetkonzern erleichtere aber die andauernden Rechtsverletzungen und den Bruch der sich dagegen wendenden Anordnungen des Gerichts durch die Beklagte. Der Supreme Court müsse sich daher den „Realitäten des E-Commerce anpassen mit seinem Potenzial für Missbrauch durch diejenigen, die das Eigentum anderer nehmen und es durch das grenzenlose elektronische Web" verkauften. Der Konzern hat aber angekündigt, in die Revision gehen zu wollen (Krempl, Kanadisches Urteil: Google muss Links löschen, www.heise.de 18.06.2014).

USA

NSA überwacht Tor-Knoten

Nach Recherchen eines internationalen Teams im Auftrag von NDR und WDR ist Sebastian Hahn, ein 27-jähriger Student und Mitarbeiter am Informatiklehrstuhl in Erlangen nach Kanzlerin Angela Merkel der zweite namentlich bekannte Deutsche, der von der NSA direkt ausgespäht wurde. Neben seinem Studium und seiner wissenschaftlichen Arbeit engagiert sich Sebastian Hahn für das so genannte Tor-Netzwerk, einen Anonymisierungsdienst. Für die Geheimdienste ist Tor ein Problem, weil der Dienst es erheblich erschwert, Menschen im Internet zu überwachen. Deshalb nutzen neben vielen NormalbürgerInnen vor allem NetzaktivistInnen, MenschenrechtlerInnen und Oppositionelle in Diktaturen das Netzwerk, aber auch Drogenhändler, Waffenschieber und andere Verbrecher, die über Tor anonym im Netz unterwegs sein wollen. Sebastian Hahn ist kein extremer Aktivist, wohl aber beharrt er auf seinen Bürgerrechten. Seit einigen Jahren wird das Tor-Netzwerk diffamierend mit dem „Darknet" gleichgesetzt. Netzaktivisten sehen in Tor aber vor allem eine Möglichkeit für Normalbürger, sich vor Überwachung zu schützen.

Sebastian Hahn gehört zu Tor-Aktivisten, die das Netzwerk betreiben. In der Nähe von Nürnberg betreibt er einen der Server des Anonymisierungsnetzwerks. Die Kennziffer von Hahns Server tauchte nun tief in Daten des NSA-Spähprogrammes XKeyscore auf. Diese unscheinbare Folge von Ziffern und Satzzeichen ist im digitalen Netz

so viel wie ein automatisch erstellter Fahndungsidentifikator. Kenntnisreiches Studium von XKeyscore zeigt, dass schon vermeintlich banale und in ihrer Natur demokratische Handlungen im Internet genügen, um jeden unabhängig von Ansehen und Herkunft seiner Person im Netz der NSA als Verdächtigen zu brandmarken. Eine Konsequenz kann sein, sich mit Anonymisierung im Netz zu schützen. Denn nur wenn das verdächtige Verhalten zum gesellschaftlichen Standard wird, kann es nicht länger verdächtig sein (Kreye, Wer sich schützt, ist verdächtig, SZ 04.07.2014, 11).

USA

NSA scannt Netz nach Gesichtern

Die National Security Agencsy (NSA), der US-amerikanische Geheimdienst für Datensammelei, scannt Mails, Textnachrichten, soziale Netze wie Facebook sowie Videokonferenzen und andere Kommunikationswege auch nach Fotos, um diese mehrere Millionen Bilder durch ihre Gesichtserkennungs-Software „Tundra Freeze“ zu schicken. Von den täglich abgefangenen mehrere Millionen Bildern seien rund 55.000 verwertbar. Dies sei ein enormes bislang unerschlossenes Potenzial, schrieb die Agency schon 2011, wie aus neuen Dokumenten des Whistleblowers Edward Snowden hervorgeht.

Die Gesichtserkennungssoftware könne Personen auch erkennen, wenn sie ihre Frisur veränderten. An anderer Stelle räumt die NSA jedoch ein, dass Bärte das Programm verwirren könnten. Die NSA hat die Gesichtserkennungs-Software seit rund vier Jahren im Einsatz. In dieser Zeit sei das Vertrauen in die Technik stark gewachsen. Die Agency werde in Zukunft nicht mehr nur die schriftliche und mündliche Kommunikation überwachen, sondern auch die Erkennung von Gesichtern, Fingerabdrücken und anderen Merkmalen zur Erkennung von Terroristen oder anderen Zielen der NSA nutzen. Eine NSA-Sprecherin wollte sich nicht dazu äußern, ob der Dienst Zugang zu der Datenbank des US-Außenministeriums hat, in der Bilder zu Visa-Anträgen gespeichert werden, und ob er Fotos aus Online-Netzwerken abgreife. Unklar ist, wie viele Menschen bereits in der Foto-Datenbank der NSA erfasst sind. Während die Gesetzeslage in den USA die NSA zwingt, sich die Speicherung von Fotos amerikanischer Staatsbürger durch ein Gericht genehmigen zu lassen, ist die Speicherung von Fotos von Bürgern anderer Länder laut US-Recht erlaubt (NSA durchsucht das Netz nach Gesichtern, www.heise.de 01.06.2014; NSA sammelt Millionen Fotos, SZ 02.06.2014, 6).

USA

Google stoppt hochsensible E-Mail auf Wunsch des Absenders

Geheime Informationen der US-Investmentbank Goldman Sachs haben durch einen Tippfehler zu Google gefunden. Goldman-Sprecherin Andrea Raphael teilte mit, dass Google die falsch adressierte E-Mail der Bank mit vertraulichen Kundendaten blockiert hat. „Google ist unserer Bitte nachgekommen, den Zugang zu der Mail zu blockieren.“ Google zufolge hatte der Empfänger bis dahin nicht auf den Inhalt zugegriffen. Damit liege keine Datenschutzverletzung vor. Wie viele Kunden betroffen waren, wurde nicht bekannt gegeben. Goldman hatte sich zuvor an ein Gericht in New York gewandt, um Google zur Blockierung der Mail zu zwingen. Die Bank verlangte auch Aufklärung darüber, wer Zugriff auf die Daten gehabt haben könnte.

Ein Mitarbeiter einer Vertragsfirma hatte die Mail versehentlich an eine falsche Adresse versendet. Goldman Sachs zufolge wollte der externe Mitarbeiter die Informationen an einen firmeneigenen Account mit der Domain gs.com schicken. Die Mail landete aber auf einem Google-Konto. Diese sind über die Endung gmail.com erreichbar. Eine Entscheidung des Gerichts steht noch aus. Laut Goldman Sachs hatte Google mitgeteilt, die Mail nicht ohne Gerichtsbeschluss löschen zu können (Google blockiert falsche Mail von Goldman Sachs, SZ 04.07.2014, 21; Google sperrt Goldman-Sachs-Irrläufer, www.welt.de 04.07.2014).

USA

Hundertausende unter Terrorverdacht

Bereits Ende Juli 2014 war ein Regelbuch bekannt geworden, mit dem die USA die Liste der Terror-Verdächtigen füllen. Neue Veröffentlichungen von Datenbanken belegen nun das Ausmaß der Datensammlungen und den Umfang der Datenbanken mit Terror-Verdächtigen. Gemäß neuer Enthüllungen von The Intercept des US-Journalisten und Snowden-Helfers Glenn Greenwald werden in Datenbanken namentlich hunderttausende Menschen als reale oder mutmaßlichen Terroristen gespeichert. In einem ausführlichen Artikel enthüllen die Intercept-Autoren, dass die CIA ein Programm namens „Hydra“ nutzt, das im Verborgenen Datenbanken anderer Staaten durchsucht und absaugt.

Die neuen Dokumente, die das Ausmaß der Terror-Überwachung in den USA belegen, stammen nicht von Edward Snowden, sondern aus „einer Quelle in der Geheimdienstgemeinde“. Auf einem veröffentlichten Dokument wird als Datum „August 2013“ angegeben, also ein Zeitpunkt, zu dem Snowden schon längst auf der Flucht war.

Die größte von The Intercept veröffentlichte Datenbank namens „Terrorist Identities Datamart Environment“ (Tide) enthalte etwa eine Million Namen, mehr als doppelt so viel wie noch 2011. Die US-Behörden haben auch Tausende US-Amerikaner im Visier. Die meisten von ihnen leben demnach in den Großstädten New York, Houston, San Diego und Chicago – aber auch in Dearborn, einem 98.000-Einwohner-Vorort von Detroit, in dem besonders viele Muslime leben. Auf einer speziellen „Watchlist“, die aus dieser Datenbank resultiert, befinden sich knapp 700.000 Personen. Die gesammelten Datenmengen seien nach dem vereitelten Sprengstoffattentat des „Unterhosen-Bombers“ auf ein US-Flugzeug beim Landeanflug auf Detroit Weihnachten 2009 sprunghaft angestiegen. Jeden Tag wüchsen die Datenbanken um etwa 1.000 Datensätze.

Eine Datenbank mit biometrischen Daten, u. a. Fingerabdrücken und Fotos, enthält 130.000 Personen. 62.794 Menschen werden beobachtet, weil sie den Taliban nahestehen sollen, 21.199 der Hamas und 11.275 der kolumbianischen Guerilla. Waren es 2001 lediglich 16 Menschen, die in Amerika kein Flugzeug besteigen durften, so sind es heute 47.000 – mit steigender Tendenz. Der Anteil von Personen, deren Verdächtigung durch keine bekannte Zugehörigkeit zu Terrorgruppen bestätigt wird, ist hoch: Es sind 280.000 von insgesamt 680.000 auf der Watchlist aufgeführten Personen (Hesse/Obermaier, USA: Hundertausende unter Terrorverdacht u. Obermaier, Der nächste Whistleblower, SZ 07.08.2014, 1, 6; Hunderttausende in Datenbank mit Terror-Verdächtigen: USA fürchten weiteren Geheimdienst-Enthüller, www.heise.de 06.08.2014).

USA

Internet-Dienste durchsuchen nach Kinderpornografie

I. Aktuelle Fälle

Google und Microsoft durchsuchen E-Mails und Clouds automatisch auf Kinderpornografie und geben damit US-Behörden Hinweise. Die Presse berichtete, dass Microsoft Informationen über einen Mann, in dessen Cloudspeicher OneDrive ein Bild abgelegt war, das offenbar in einschlägigen Datenbanken mit bekannten Abbildungen von Kindesmissbrauch auftaucht, an die sogenannte Cyber Tipline des US-amerikanischen National Center for Missing and Exploited Children (NCMEC) weitergegeben hat. Die Organisation informierte ihrerseits die Polizei. Der Mann wollte anschließend offenbar über seinen Live.com-E-Mail-Account zwei weitere Bilder verschicken. Am 31.07.2014 wurde der Mann festgenommen. Er gestand, einschlägige Bilder über „ein Mobilfunkgerät“ mit anderen ausgetauscht zu haben. Er habe dazu eine Chat-App namens Kik-Messenger benutzt.

US-Polizeibeamte bestätigten, dass es weitere Fälle gebe, in denen „Internetanbieter“ ähnliche Details weitergegeben haben. Kurz zuvor war bekannt geworden, dass in den USA ein weiterer Mann aufgrund von Bildern sexuellen Missbrauchs an Kindern in seinem Gmail-Account verhaftet worden war. Google waren drei kinderpornografische Bilder im Gmail-Postfach des Täters aufgefallen. Vermutlich schlug ein automatisches Warnsystem auf ein als problematisch bekanntes Bild an. Über das US-amerikanische NCMEC wurde die Polizei vor Ort informiert, die den Mann festnahm. Bei einer anschließenden Hausdurchsuchung fanden die Beamten auf dem Telefon und dem Tablet-Computer des Mannes mutmaßlich kinderpornografisches Material; ebenso entdeckten sie Textnachrichten, in denen er sich über sein Interesse an Kindern auslässt. Videoaufnahmen sollen außerdem Kinder zeigen, die mit ihren Familien das Fastfood-Restaurant besuchten, in dem der Mann als Koch arbeitet. 1994 war der Verdächtige bereits wegen sexuellen Missbrauchs an einem achtjährigen Kind verurteilt worden. Ein Prozess soll nun die neuen Vorwürfe klären.

II. Hashwert-Abgleich

Googles PR-Agentur verwies in diesem Zusammenhang auf einen Gastbeitrag, den der Chefjustiziar des Unternehmens, David Drummond, 2013 für den britischen „Telegraph“ verfasst hatte. Darin ist nicht von E-Mail-Anhängen die Rede, sondern von Googles Bemühungen, Bilder, die sexuellen Missbrauch an Kindern zeigen, aus den Suchergebnissen zu entfernen. Erwähnt wird zudem eine Technik, die auch im vorliegenden Fall eine Rolle gespielt haben könnte: „Seit 2008 nutzen wir eine ‚Hashing‘-Technologie, um bekannte Missbrauchsbilder zu markieren, so dass wir Kopien dieser Bilder an anderer Stelle identifizieren können.“ Dazu erstellt das Unternehmen sogenannte Hashwerte, mathematische, eindeutige Abstraktionen von Bildern. Diese Hashwerte und der jeweilige Algorithmus, um aus Bildern diese Hashwerte zu erstellen, können öffentlich zugänglich gemacht werden. Andere Software-Hersteller, aber auch staatliche Einrichtungen, Forschende und Nichtregierungsorganisationen, können so die Google-Datenbank zur Kinderpornografie für eigene Lösch- und Blockierzwecke benutzen, ohne selbst mit dem strafbaren Material in Berührung zu kommen.

Folgendes Szenario ist wahrscheinlich: Der Täter versendet ein Missbrauchsbild über Googles Maildienst. Google gleicht automatisch alle über Google-Dienste verschickten Bilder mit einer Datenbank von digitalen Fingerabdrücken bekannter Missbrauchsbilder ab. Bei einem Fund wird das NCMEC gewarnt, das den Fall beurteilt und die Polizei informiert. In einem im November 2013 bekannt gewordenen Fall war ein Kalifornier festgenommen worden, der kinderpornografische Fotos in Googles Fotodienst Picasa gespeichert hatte. Auch Microsoft betreibt Datenbanken mit Hashwerten bekannter kinderpornografischer Abbildungen. Aufgrund von Selbstverpflichtungen und öffentlichem Druck setzen immer mehr Internet-Dienstleister auf solche Systeme. Facebook und Twitter etwa nutzen PhotoDNA, Microsofts Kinderpornografie-Datenbank. Der Nutzen solcher Systeme ist allerdings streitig. Es besteht zudem die Gefahr, dass sie missbraucht werden, um Inhalte zu sperren oder Personen und Firmen gezielt in Misskredit zu bringen.

III. Die Sichtweise der Unternehmen

Es gibt unterschiedliche Ansichten darüber, ob ein Unternehmen – ob automatisiert oder nicht – generell in den Postfächern seiner KundInnen stöbern darf. Im März 2014 wurde Microsoft mit Spionagevorwürfen konfrontiert, weil das Unternehmen im Rahmen interner Ermittlung ohne Gerichtsbeschluss das Hotmail-Postfach eines Bloggers ausgespäht hatte.

In Googles deutschen Nutzungsbedingungen heißt es: „Mit der Nutzung von Google-Services erkennen Sie an und stimmen zu, dass Google Informationen zu Ihrem Konto und den mit diesem Konto verbundenen Content möglicherweise aufruft, erhält oder weitergibt, wenn dies aus rechtlichen Gründen erforderlich ist oder Google sich in gutem Glauben befindet, dass der Zugriff auf diese Informationen, die Beibehaltung oder die Weitergabe notwendig sind.“ Google bekräftigte aktuell, dass nach Hinweisen auf andere Verbrechen, etwa Mord oder Vergewaltigungen, nicht gesucht werde. Kinderpornografie sei ein Sonderfall. Google betont auch immer

wieder, dass Nutzende des E-Mail-Dienstes nicht davon ausgehen könnten, dass ihr Schriftverkehr privat sei. In Gerichtsunterlagen verglich der Konzern E-Mail mit Geschäftsbriefen, die auch von der Assistentin des Empfängers geöffnet werden können. In einer Stellungnahme schrieben Google-Juristen im Jahr 2013, dass sie vom Briefgeheimnis nichts hielten. Aus ihrer Sicht könne „eine Person keine legitime Erwartung haben, dass Informationen privat bleiben, die sie freiwillig an Dritte weitergibt“. Andere Anbieter wie Yahoo und Apple haben ähnliche Bedingungen wie Google.

Microsoft teilte im Zusammenhang mit dem aktuellen Fall mit: „2009 haben wir dabei geholfen, PhotoDNA zu entwickeln, eine Technologie, die dazu dient, die Ausbreitung von Bildern missbrauchter Kinder zu unterbrechen, über die wir dem National Center for Missing and Exploited Children berichterstatten, wie das Gesetz es vorsieht.“ In Microsofts US-Nutzungsbedingungen steht explizit: „Wir setzen automatisierte Technologien ein, um Kinderpornografie oder missbräuchliches Verhalten aufzuspüren, das unseren Systemen, unseren Kunden oder anderen schaden könnte.“

IV. Die Praxis in Deutschland

Betroffen von den Unternehmens-Durchsuchungen sind auch deutsche Konten. Ralf Bremer, Sprecher von Google in Deutschland, erklärte: „Alle Nutzerkonten werden hier gleichbehandelt.“ Für Microsoft bestätigte Sprecher Thomas Baumgärtner, dass die Daten deutscher Nutzender ebenso durchsucht werden: „Es ist wie an der Haustür einer großen Mietanlage“. Was an Bildern rein- und rauskomme, werde automatisch mit einer Datenbank abgeglichen. Deutsche Provider wie GMX, Web.de, Telekom und Freenet mit der Initiative „E-Mail made in Germany“ durchsuchen die Inhalte ihrer Nutzenden nur nach unerwünschter Werbung und nach Computerschädlingen. GMX bestätigte: „Eine inhaltliche Überwachung der E-Mails halten wir nicht für vereinbar mit deutschem Datenschutz.“

Das anlasslose inhaltliche Schnüffeln in den Mails ist nicht nur deutschen Providern verboten, sondern auch US-Diensten wie Gmail. Betroffen sind nicht nur die KundInnen von Unternehmen wie Microsoft und Google selbst, sondern auch alle, die an ein solches Postfach eine Botschaft gesendet haben. Möglich ist auch, dass eine E-Mail nicht direkt adressiert, aber z. B. an ein Gmail-Konto weitergeleitet wird.

In Deutschland lobte die hessische Justizministerin Eva Kühne-Hörmann „den wertvollen Beitrag“, wenn Internetdienste ihr „Stillschweigen“ brächen. Die Bundesdatenschutzbeauftragte Andrea Voßhoff äußerte sich kritischer: Das systematische Scannen von Mail-Nachrichten sei ein „massiver Eingriff in das durch das Grundgesetz garantierte Recht des Fernmeldegeheimnisses sowie in das Recht auf informationelle Selbstbestimmung“. Der auf IT-Recht spezialisierte Anwalt Udo Vetter erläuterte: „Die unaufgeforderte Hilfe für Strafverfolgungsbehörden, wie von Gmail praktiziert, wäre von deutschem Recht nicht gedeckt. Bei Verstößen gegen das Fernmeldegeheimnis droht eine Haftstrafe von bis zu fünf Jahren.“

Wie heißt es in Artikel 12 der Allgemeinen Erklärung der Menschenrechte der UNO von 1948? „Niemand darf willkürlichen Eingriffen ... in seinen Schriftverkehr ausgesetzt werden“ (Becker/Brauck/Schindler/Schmundt/Schulz, Die Hilfssheriffs, Der Spiegel 33/2014, 126 f.; Verdächtiger nach Hinweis von Microsoft festgenommen, www.spiegel.de 07.08.2014; Google-Hinweis führt zu Festnahme, www.spiegel.de 04.08.2014).

USA

Google Baseline sucht „biochemischen Fingerabdruck“ der Gesundheit

In einem viele Millionen Dollar schweren Projekt „Baseline“ will Google die körperlichen Schwächen von 175 ProbandInnen durchleuchten. Ihr Erbgut soll vom ersten bis zum letzten Basenpaar sequenziert und in Googles Rechenzentrum gespeichert werden. Zudem sammeln Forschende der US-Elite-Universität Stanford und Duke für Google von den Teilnehmenden viele Körperdaten, untersuchen u. a. ihr Blut, ihre Spucke, ihren Urin und ihre Tränenflüssigkeit. Sie wollen herausfinden, wie die Körper unter Anstrengung reagieren, wie gut sie Nahrung verwerten. Zusammen mit den Krankengeschichten der Eltern entsteht ein präzises Bild der 175 Individuen.

Ziel von Baseline ist es, den „biochemischen Fingerabdruck“ gesunder Personen zu erstellen: „Wir wollen verstehen, was es heißt, gesund zu sein, bis hinunter zur molekularen und zellulären Ebene“. Auf lange Sicht wollen die Forschenden in den Daten auch frühe Hinweise auf Krankheitsrisiken finden. Per Datenanalyse sollen verborgene Muster aufgedeckt, und möglicherweise Krebs oder Diabetes prognostiziert werden. Nach diesem Pilotversuch sollen sich tausende weitere ProbandInnen auf die gleiche Weise durchleuchten lassen. Baseline ist ein sog. „Moonshot“ Googles, ein Projekt mit hohem Risiko und potenziell hohem Gewinn.

Markus Nöthen, Direktor des Instituts für Humangenetik an der Uni Bonn meinte: „Für mich ist Baseline kein aussichtsloses Unterfangen. Mit Google steigt jetzt erstmals ein Privatfirma in diese bislang öffentlich finanzierte Forschung ein. Es ist beeindruckend zu sehen, wie viele Daten auf einmal der Konzern sammeln will.“ Es gebe schon einige ähnliche Langzeitstudien, die viele Körperdaten von einer großen Anzahl Menschen sammeln, etwa die Kora-Studie des Helmholtz-Zentrums München, oder die europäische Epic-Studie, die Zusammenhänge zwischen Krebs und Ernährung untersucht. Google verfüge über das Wissen, die Daten auch auszuwerten.

Ausgewertet werden die Daten von Gesunden, was Humangenetiker Peter Propping kommentiert: „Daraus etwas über Krankheiten zu lernen, wird die große Schwierigkeit sein.“ Dazu brauche man eine sehr große Stichprobe – die jetzt beginnende „Nationale Kohorte“ in Deutschland will ca. 200.000 Menschen untersuchen. Zudem müsse man diese Personen über einen sehr langen Zeitraum begleiten, so Nöthen: „Solche Studien zeigen erst nach 20 bis 30 Jahren ihren Wert.“ Dann treten auch bei den einstmals Gesunden die ersten Krankheiten auf und erst dann wird möglicherweise klar, wodurch sie sich hätten vorbeugen lassen (Behrens, Der Google-Mensch, SZ 26./27.07.2014, 25).

Technik-Nachrichten

Internet-Spionage mit „Canvas Fingerprinting“

Mit einer neuen Methode, dem „Canvas Fingerprinting“, verfolgt die Werbewirtschaft das Ziel der eindeutigen Identifikation von Rechnern, ohne dass die Betroffenen sich hiergegen zur Wehr setzen können. Im Gegensatz zu normalen Cookies können sie „Canvas Fingerprinting“ nicht blockieren. Auch deutsche Seiten setzen verstärkt auf diese Art der Verfolgung von Internet-Aktivitäten. „Canvas Fingerprinting“ nutzt die Profilinformationen des Browsers der Nutzenden, die an die Webseite gesendet werden, um sie im Netz zu identifizieren. Das sind beispielsweise die installierte Schriftart, die Hardware oder die eingestellte Zeitzone. Daraus erstellt die Seite ein unsichtbares Bild in einem HTML-Canvas-Element – daher der Name. Ein Canvas-Element dient dazu, einfache Grafiken auf einer Webseite anzuzeigen. Aus dem unsichtbaren Bild wird dann ein einzigartiger Code generiert, der die Nutzenden im Netz verfolgt und identifiziert. Für die Verbreitung der umstrittenen Technik ist vor allem die Firma AddThis verantwortlich, die Facebook- und Twitter-Buttons auf 13 Mio. Internetseiten zur Verfügung stellt. Zumindest auf einem Teil dieser Internetseiten hat das Unternehmen zwischen den Buttons ihre Canvas-Fingerprinting-Technik versteckt.

Wissenschaftler der US-amerikanischen Princeton-Universität und der belgischen Katholischen Universität Leuven haben schon auf 5% der beliebtesten Webseiten die Technik entdeckt. Genutzt wird die Technik von Nachrichtenseiten, Regierungswebseiten und Erotikportalen – also im Prinzip überall. In Deutschland sind das beispielsweise t-online.de, n-tv.de oder computerbild.de. Eine Auflistung findet sich unter http://is.gd/k4ezEv. Die Technik kann von einem durchschnittlichen Nutzenden nicht bemerkt und kaum verhindert werde. Das Abschalten der Java-Script-Funktion hilft; dann funktionieren aber viele Seiten nicht mehr richtig. Während Cookies auf dem Nutzer-Rechner gespeichert werden, wird der Canvas-Code direkt an die Server der Webseiten übermittelt. Die NGO Electronic Frontier Foundation entwickelt bereits erste Ansätze, um der fiesen Methode einen Riegel vorzuschieben. Das Addon „Privacy Badger“ für Firefox und Chrome könnte Canvas Fingerprinting in Zukunft blockieren (Boie, Schlimmer als Cookies, SZ 23.07.2014, 1; Dieser unlöschbare Cookie verfolgt Sie im Netz, www.focus.de 23.07.2014).

Skybox liefert Google Echtzeit-Satellitenbilder

Google hat das Satellitenbild-Startup Skybox für 500 Millionen US-Dollar erworben und stärkt seine digitalen Kartendienste mit der Übernahme von Skybox Imaging, das Bilder aus dem All in hoher Auflösung erstellt. Es gehe darum, „Google Maps präzise zu halten mit Bildern, die auf dem neuesten Stand sind“.

Skybox bietet seinen Kunden das Beobachten gewünschter Gebiete mit detailreichen Fotos und 90 Sekunden langen Videos an. Als Dienstleistungen nennt Skybox z. B. die Überwachung von Feldern auf Schädlingsbefall und die Aufsicht über Energie-Pipelines. Auch die Auswertung der Container-Bewegungen in Häfen, der Aktivität auf Flughäfen oder der Bestände auf Parkplätzen von Autohändlern ist möglich. Außerdem will Google damit die Versorgung mit Internet-Zugängen und die Hilfe bei Unglücken und Naturkatastrophen verbessern. Ende 2013 lieferte es als erstes kommerzielles Unternehmen ein vom Weltraum aufgenommenes HD-Video. Die Satelliten sollen fahrende Autos nahezu in Echtzeit erkennen. Laut Mitarbeiterschaft soll z. B. folgende Frage beantwortet werden können: Wie viele Autos stehen derzeit auf den Parkplätzen von sämtlichen Wal-Mart-Firmen in den USA? Google ist selbst bei der Entwicklung digitaler Satellitenkarten mit seinem Projekt Google Earth weit vorangekommen. Etablierte Anbieter wie DigitalGlobe oder GeoEye haben den Erdball erfasst, Skybox verspricht frischere Bilder auf Bestellung.

Skybox will als einer von mehreren neuen Anbietern von drastisch gesunkenen Kosten für die Entwicklung und Herstellung von Satelliten profitieren. Die Technik wird in deutlich kleinere Satelliten gesteckt, als man sie früher baute. Die Skybox-Satelliten sind nach bisherigen Berichten nur rund 100 Kilogramm schwer. Die Kosten pro Satellit werden auf rund 25 bis 50 Millionen Dollar geschätzt. Skybox selbst meinte in seiner Erklärung zur Übernahme durch Google, man habe die bislang kleinsten Satelliten für hochauflösende Bilder gebaut. Skybox startete im Jahr 2009. Mitgründer Dan Berkenstock verkündete bereits früh die Vision, man wolle jedem die Möglichkeit geben, jederzeit zu sehen, was überall auf der Welt passiere. Skybox will dafür über die Jahre rund zwei Dutzend Satelliten ins All bringen, steht bei dem Plan aber erst am Anfang. Bisher bekommt Google seine Satellitenaufnahmen von Digital Globe. Erst Februar 2014 hatte Google einen neuen „mehrjährigen Vertrag“ unterschrieben (Tandriverdi, Luftbilder live, SZ 12.06.2014, 17; Kuri, Google kauft Satellitenbild-Startup Skybox für 500 Millionen Dollar, www.heise.de 11.06.2014).

Soziale Medien

Facebook experimentiert mit Mitgliedern

Facebook forscht schon seit längerem mit den Daten seiner Nutzenden. Aktuell wurde ein Psycho-Experiment bekannt, bei dem die Newsfeeds von mehreren 100.000 Usern der englischsprachigen Facebook-Version manipuliert worden sein sollen. Facebook hat das heftig kritisierte Psycho-Experiment verteidigt. Für das Online-Netzwerk sei es wichtig zu verstehen, wie Mitglieder auf verschiedene Inhalte reagierten: „Wir überlegen vorsichtig, welche Forschung wir betreiben, und haben ein striktes internes Aufsichtsverfahren."

Bei dem einwöchigen Experiment im Januar 2012 sollte ermittelt werden, wie sich Emotionen in Netzwerken ausbreiten. Entsprechend wurden für Nutzer die Einträge ihrer Facebook-Freunde vorgefiltert: Den einen wurden mehr positive Nachrichten angezeigt, den anderen mehr negative. Die Studie ergab, dass Menschen, die mehr positive Nachrichten sahen, mehr dazu neigten, auch selbst Einträge mit positivem Inhalt zu veröffentlichen – und umgekehrt. Einer der Autoren der Studie, Adam Kramer, erläuterte in einem Facebook-Eintrag, man habe die Sorge überprüfen wollen, dass Menschen sich ausgeschlossen fühlten, wenn sie positive Nachrichten ihrer Freunde sehen. Zudem habe es zuvor Bedenken gegeben, dass viele negative Einträge von Freunden die Nutzer veranlassen könnten, Facebook zu meiden. Er räumte ein: „Wir haben unsere Motive in dem Papier nicht klargemacht." Insgesamt waren bei dem Experiment ohne Vorwarnung die Newsfeeds von 689.003 Nutzenden der englischsprachigen Facebook-Version manipuliert worden. Über drei Millionen Einträge wurden von Software ausgewertet, die per Wortanalyse die Emotion zuordnete.

Die britische Datenschutzbehörde Information Commissioner´s Office (ICO) nahm wegen der Studie Ermittlungen auf, weil es eine große Empörung über dieses Experiment gab. Die Datenschutzgruppe „Electronic Privacy Information Center" (EPIC) reichte eine Beschwerde bei der US-Handelsaufsicht FTC gegen das Psycho-Experiment ein. EPIC kritisierte, dass der Test gegen die geschäftlichen Regeln sowie gegen eine Vereinbarung mit der FTC zum Schutz der Nutzerrechte verstoßen habe. Andere Forschende kritisierten den Test, weil Facebook die Betroffenen nicht um ihre Einwilligung gebeten hat. Bei wissenschaftlichen Studien gehöre es zum ethischen Standard, den Versuchsteilnehmenden zu sagen, dass sie Teil eines Experiments werden. Das gilt auch für Studien, bei denen die Testpersonen nicht wissen sollen, was genau untersucht wird, weil sie das in ihrer Wahrnehmung beeinflussen könnte. In solchen Studien findet sowohl eine Einführung statt als auch eine Auflösung am Ende, bei der über das eigentliche Ziel informiert wird.

Facebook betonte, dass bei der Studie ein „angemessener Schutz" gewährleistet gewesen sei. Das Unternehmen könne aber verstehen, dass Menschen über diese Studie verärgert seien; in Zukunft wolle man es besser machen. Die Passage in den Geschäftsbedingungen, dass die Daten auch für Forschungszwecke genutzt werden dürfen, wurde übrigens erst nach dem Psycho-Test in die Geschäftsbedingungen eingeführt.

Schon im September 2012 wurde in der Technology Review ein Beitrag von Tom Simonite veröffentlicht, der die Sozialwissenschaftler und Netzwerktheoretiker des Unternehmens besuchte. Einer der Männer, die Firmenchef Mark Zuckerberg damals als „Schatzsucher" auserkoren hatte, war Cameron Marlow. Der hochgewachsene Experte war damals Mitte 30 und leitete gut abgeschirmt von Öffentlichkeit und Presse ein zwölfköpfiges „Data Science Team". Das Ziel der Gruppe, die Facebook damals schon verdoppeln wollte, war es, eine Art Bell Labs für das Zeitalter der sozialen Netzwerke zu schaffen: „Mithilfe von Mathematik, Programmierkunst und Erkenntnissen aus den Sozialwissenschaften sollen die Facebook-Forscher in den Datenberg vordringen und Schätze heben. Im Unterschied zu anderen wissenschaftlichen Mitarbeitern, die nur einzelne Aspekte der Online-Aktivitäten untersuchen, hat Marlows Team Zugang zum gesamten Datenbestand von Facebook." Nicht einmal die Führungsriege um Zuckerberg habe einen vergleichbaren Einblick in die persönlichen Informationen, die Millionen Facebook-Nutzer im Sekundentakt von sich preisgeben.

Bei 2012 durchgeführten Experimenten kam heraus, dass Nutzer sich mit einer um 50% höheren Wahrscheinlichkeit an Anzeigen erinnern, wenn diese erkennbar von einem Freund gutgeheißen wurden. Mit derartigen Einblicken versuchte Facebook bereits vor dem Börsengang, potenzielle Investoren zu locken: „Denn wer die Mechanik der sozialen Beeinflussung versteht, kann Online-Werbung noch eindrücklicher gestalten und damit bewirken, dass die Nutzer noch häufiger auf Anzeigen klicken." Facebook holt für seine Experimente keine Genehmigung ein. Wer die Geschäftsbedingungen akzeptiert, hat damit nach Ansicht des Konzerns automatisch seine Zustimmung zu etwaigen Untersuchungen an seinem Nutzerkonto gegeben. Lorrie Cranor, Informatikerin an der Carnegie Mellon University, die das CyLab-Labor für Usable Privacy and Security leitet, erläuterte den Unterschied zwischen den früheren und der aktuellen Untersuchung: „Was bei dieser Studie anders ist, ist die Tatsache, dass die Ergebnisse veröffentlicht wurden, ohne dass die Teilnehmer explizit der Studie zugestimmt hätten."

Das „Data-Science-Team" von Facebook hat einerseits die Optimierung des sozialen Netzwerks im Blick, andererseits auch sozialwissenschaftliche Fragestellungen. 2012 demonstrierte Facebook, wie es Menschen dazu bewegen könnte, Organe zu spenden. Der Konzern platzierte anklickbare Boxen in den Zeitleisten von Nutzern, in denen diese angeben konnten, ob sie registrierte Or-

ganspender sind. In der Folgezeit nahm die Zahl der Neuregistrierungen stark zu, wobei nicht klar ist, wie sehr auch die Berichterstattung in den Medien dazu beitrug. Facebook steht mit dieser Form von Social Engineering nicht alleine. „Besorgniserregender daran ist, dass die Praktiken von Facebook jegliche Transparenz vermissen lassen", meinte Zeynep Tufeki, Professor an der University of North Carolina in Chapel Hill. „Was macht Facebook neben diesen täglichen Experimenten sonst noch? Wir haben keine Ahnung." Und der Spiegel kommentierte: „Die Hexenmeister an den Reglern können die soziale Realität gezielt verändern. Werden sie als Nächstes die aggressiven oder boshaften Bemerkungen hochdrehen, um den Streit unter den Nutzern zu schüren?" (Facebook verteidigt umstrittenes Psycho-Experiment, www.heise.de 30.06.2014; Facebook experimentiert schon länger mit Nutzerdaten, www.heise.de 01.07.2014, Tandriverdi, Ermittlungen gegen Facebook, SZ 03.07.2014, 19, Facebook-Nutzer als Laborratten: Universitäten mischen mit, www.heise.de 04.07.2014, Datenschutz-Aktivisten gehen gegen Facebook-Experiment vor, www.heise.de 04.07.2014; Dworschak, Hexenmeister am Regler, Der Spiegel 28/2014, 114).

Google+ gibt Klarnamenpflicht auf

Das Unternehmen Google gab in einem kurzen Posting in seinem sozialen Netzwerk Google+ bekannt, dass dort die Pflicht der Nutzenden, ihre wirklichen Namen anzugeben, aufgegeben wird. Google habe mit dieser Klarnamenspflicht eine Community echter Menschen aufbauen wollen, wisse aber, dass auf diese Weise viele Menschen ausgeschlossen wurden. Im Laufe der Zeit habe das Unternehmen dann den Benutzern von Google+-Seiten erlaubt, beliebige Namen anzugeben, und YouTube-Nutzer durften ihren Namen ebenfalls zu Google+ mitnehmen – auch wenn er ein Pseudonym war. Google schreibt weiter, es sei dem Unternehmen bekannt, dass Benutzer schon länger eine Änderung der Namens-Policy wünschen. Die bisherige unklare Regelung habe zu „unnötigerweise schwierigen Erfahrungen" für einige Nutzende geführt. Dafür entschuldige sich das Unternehmen (Google+: Klarnamenspflicht entfällt, www.heise.de 16.07.2014).

Snapchat muss Datenschutz verbessern

Die US-amerikanische Behörde Federal Trade Commission (FTC) hat Anfang Mai von Snapchat gefordert, die Foto-App in Sachen Datenschutz zu verbessern – u. a. durch ehrliche Informationen. Nach Meinung der FTC sagen die Macher nicht die ganze Wahrheit über ihre App. Versprochen wird, dass sich die sog. Snaps nach wenigen Sekunden selbst löschen. Tatsächlich können diese rekonstruiert und mit einfachen Mitteln gesichert werden.

Mit Snap-Chat kann der Nutzer Fotos und Videos (sog. Snaps) verschicken. Diese sind maximal zehn Sekunden lang zu sehen. Eine sog. Snap-Story aus mehreren Snaps ist 24 Stunden lang zu sehen. Der Dienst hatte im Juni 2014 bereits 60 Millionen Nutzer und ist vor allem bei Jugendlichen beliebt. Häufig wird er für das sog. Sexting verwendet, also das Versenden von z. B. Nacktfotos. Die Daten sind also besonders sensibel.

Mit Programmen wie SnapHack oder SnapSave können heimlich Screenshots erstellt werden. Außerdem können gelöschte Snaps durch IT-Forensiker wieder hergestellt werden. Nach Ansicht der FTC muss Snapchat hierüber in den Nutzungsbedingungen informieren. Es wurde nun ein Vergleich geschlossen. Die nächsten 20 Jahre schaut dem App-Entwickler ein Datenschutz-Experte auf die Finger.

Snapchat war bereits wegen weiterer Datenschutzmängel in der Kritik. Hacker konnten Neujahr 2014 eine bekannte Schwachstelle ausnutzen und Namen und Telefonnummern von 4,6 Millionen Nutzern im Internet veröffentlichen. Außerdem wurden durch Snapchat ohne vorherige Information Standort- und Adressbuchdaten von Nutzern gesammelt.

(Snapchat lehnt Milliarden-Offerte von Facebook ab, www.zeit.de, 14. November 2013; Snapchat muss nachbessern, www.zeit.de, 09. Mai 2014; Kroker, Social Media 2014: Die Zahlen zu Facebook, Twitter, Instagram, Pinterest, Vine & Snapchat, www.blog.wiwo.de, 12. Juni 2014)

BND und Bundeswehr planen „Echtzeit"-Überwachung sozialer Netzwerke

Wie Ende Mai/Anfang Juni bekannt wurde, wollen der Bundesnachrichtendienst und die Bundeswehr künftig auch soziale Medien wie Facebook und Twitter beobachten. In den Streaming-Daten sollen mit statistischen Verfahren Trends und Auffälligkeiten erkannt werden. Ziele sind die Früherkennung von Entwicklungen im Ausland bzw. die Abwehr von Gefahren. Das Bundesinnenministerium hat die viel kritisierten Pläne nun verteidigt. Das Vorhaben sei grundrechtskonform; ein Eingriff in das von Artikel 10 geschützte Brief- sowie Post- und Fernmeldegeheimnis liege nicht vor, da öffentliche Informationen ausgewertet würden.

Innenstaatssekretär Ole Schröder schrieb hierzu am 22. Juli 2014 an Andrej Hunko (Die Linke): „Es liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter eingrenzbaren Personenkreis richten." Eine Auswertung der Daten einzelner Nutzer sei nicht das Ziel. Außerdem sollten Daten nicht gespeichert, sondern der laufende Datenfluss beobachtet werden.

Andrej Hunko sagte hierzu: „Wenn eine Verfolgungsbehörde Daten über eine bestimmte Person zusammenträgt, braucht es dazu eigentlich einen richterlichen Beschluss." Werde dies von Geheimdiensten und Militärs nach Gutdünken praktiziert, gehe „das Vertrauen in die Privatsphäre der digitalen Kommunikation vollends verloren".

Auch Bundesjustizminister Heiko Maas sprach sich gegen die geplante Echtzeitüberwachung aus. „Es gibt da ganz klare Grenzen: Auch Geheimdienste müssen sich an die Gesetze halten. Für eine Totalüberwachung aller sozialen Netzwerke in Echtzeit sehe ich keine rechtliche Grundlage", sagte Maas gegenüber der Passauer Neuen Presse.

Aus Unterlagen der Bundesregierung geht hervor, dass das Verteidigungsministerium im Mai 2014 ein Forschungsprojekt mit dem Fraunhofer Institut und dem US-Konzern IBM gestartet hat. Ziel des Vorhabens „WeroQ" ist die „Wissenserschließung aus offenen Quellen". Es soll erforscht werden, welche Technologien zur IT-gestützten Nachrichtengewinnung aus offenen Quellen für die Bundeswehr nutzbar sind. Damit soll in den Einsatz- und Interessengebieten der Bundeswehr eine „belastbare Erfassung von Meinungs- und Stimmungslagen der Bevölkerung" ermöglicht werden. Das Forschungsvorhaben soll planmäßig zwei Jahre dauern und einen Etat von 1,35 Millionen Euro verschlingen. Basis des Vorhabens soll die Geschäftssoftware „IBM Content Analytics" sein. Diese kann laut Internetseite von IBM wertvolle von wertlosen Inhalten unterscheiden und Kundenpräferenzen ermitteln. Die Analysetools Textrapic und Brandwatch werden bereits von dem Zentrum Operative Kommunikation der Bundeswehr eingesetzt, um das sogenannte Informationsumfeld bei Auslandseinsätzen aufzuklären. Beide Programme werten sämtliche verfügbaren öffentlichen Quellen aus und damit auch soziale Netzwerke.

Die Pläne des Bundesnachrichtendienstes sind Teil der sogenannten Strategischen Initiative Technik (SIT), für die 300 Millionen Euro ausgegeben werden sollen. Laut vertraulichen Unterlagen, die der Süddeutschen Zeitung, dem NDR und dem WDR vorliegen, liegt ein besonderer Schwerpunkt der Initiative auf der Echtzeitüberwachung sozialer Netzwerke. Das Teilprojekt nennt sich „Echtzeitanalyse von Streaming-Daten". So sollen Stimmungen in der Bevölkerung ausländischer Staaten gemessen und sofort in BND-Lagebilder einfließen.

(Goetz/Leyendecker/Obermaier, BND will soziale Netzwerke live ausforschen, www.sueddeutsche.de, 20. Mai 2014; Fuchs, Bundeswehr will soziale Netzwerke überwachen, www.zeit.de, 02. Juni 2014; Wilkens, Justizminister: Keine Echtzeit-Überwachung von Facebook und Twitter durch BND, www.heise.de, 11. Juli 2014; Innenministerium verteidigt Überwachung sozialer Netzwerke, www.zeit.de, 25. Juli 2014; Holland, Bundeswehr nutzt soziale Medien zur Aufklärung von Stimmungslagen, www.heise.de, 25. Juli 2014)

Facebook soll Bank-Lizenz beantragt haben

US-Medien zufolge soll Facebook in Irland eine Banklizenz beantragt haben – voraussichtlich zum Handeln mit „E-Money". Facebook hat dies bislang nicht bestätigt. Zu Gerüchten nehme man grundsätzlich keine Stellung, teilte eine Facebook-Sprecherin mit. Angestrebt wird aber dem Vernehmen nach, ein „Micropayment-System" zu etablieren. Hiermit könnten sich die 1,3 Milliarden Facebook-Freunde untereinander Geld anweisen. Denkbar sind virtuelle Zahlungsvorgänge nach dem Modell von PayPal.

Ins Bild passt die Anstellung von David Marcus, Ex-Chef des Online Bezahldienstes PayPal, als neuen Manager für Messenger-Dienste bei Facebook. Marcus verließ PayPal am 27. Juni, um zu Facebook zu wechseln. Marcus könnte den Facebook-Messenger zukünftig so erweitern, dass Facebook-Nutzer dort u. a. Konzerttickets kaufen können, wie Analyst Brian Blau von der Beratungsfirma Gartner äußerte. „Angesichts seiner Expertise in den Bereichen E-commerce und Zahlungsverkehr ist es naheliegend, dass er viele dieser Dinge bei Facebook einführen wird."

Die Justiz-Kommission der EU hat bereits Datenschutzbedenken geäußert. Bankdaten und gleichzeitig Informationen aus E-Mails und Beiträgen auszuwerten und möglicherweise zu kreuzen, dürfte nicht mit den Prinzipien des Datenschutzes vereinbar sein, sagte eine Kommissionssprecherin. Zuständig für die Erteilung der Lizenz ist Irlands Zentralbank. Dort ist zu erfahren, dass „die Art, wie persönliche Daten genutzt werden, sehr wohl Auswirkungen auf die Erteilung einer Banklizenz haben kann. Die irische Datenschutzbehörde fühlt sich eher nicht zuständig, vorbehaltlich eines Gesprächs mit Facebook, dessen Pläne man offiziell nicht kenne, sagte eine Sprecherin.

(Facebook beantragt Bank-Lizenz in Irland, www.deutsche-wirtschafts-nachrichten.de, 10. Juni 2014; Cáceres, Facebooks Bank-Pläne alarmieren Datenschützer, www.sueddeutsche.de, 12. Mai 2014)

Rechtsprechung

US-Supreme Court

Smartphone-Durchsuchung nur mit richterlicher Anordnung

Der Supreme Court, das höchste US-Gericht hat, mit Urteil vom 25.06.2014 mit allen neun Richtern einstimmig die Durchsuchung von Handys durch die Polizei drastisch beschränkt (Riley v. California, US v. Wurie). Demnach dürfen Handys von Festgenommenen nur nach einem richterlichen Beschluss durchforstet werden. Der Supreme Court begründete dies mit dem Hinweis, dass Mobiltelefone heute ein wichtiger Bestandteil der Privatsphäre darstellten. Daher seien die Daten entsprechend zu schützen: „Die Polizei darf ohne Gerichtsbeschluss grundsätzlich nicht digitale Informationen auf Mobiltelefonen von Personen durchsuchen, die festgenommen wurden. ... Moderne Mobiltelefone sind nicht einfach eine weitere technologische Annehmlichkeit. ... Mit all dem, was sie enthalten und was sie enthüllen könnten, bedeuten sie für viele Amerikaner ‚die Privatsphäre des Lebens'." Gemäß der Entscheidung dürfen Polizeibeamten zwar ein Smartphone öffnen und überprüfen, ob sich darin etwa eine Rasierklinge befindet. Die im Telefon gespeicherten Daten könnten aber niemanden gefährden. Auch könne die Polizei verhindern, dass Beweise vernichtet werden, indem sie die Batterie entferne, das Gerät abschalte oder in eine Aluminiumfolie packe, damit ein Hacker aus der Ferne keine Daten löschen könne. Die inhaltliche Durchsuchung der Informationen setze jedoch einen richterlichen „warrant" voraus. Die Entscheidung bezieht sich auf zwei Fälle, in denen die Polizei Daten, Videos und Fotos auf Handys von Festgenommenen sichtete, was später zu einer Verurteilung führte.

Der Vorsitzende John Roberts spannte in seiner Begründung einen Bogen von den Gründungstagen der USA bis in die Gegenwart, um die Bedeutung von Mobiltelefonen für den modernen Menschen hervorzuheben: Die Geräte seien „ein solch beherrschender und vereinnahmender Teil des täglichen Lebens, dass der sprichwörtliche Besucher vom Mars sie für ein wichtiges Merkmal der menschlichen Anatomie halten könnte." Die Richter begründeten ihr Urteil mit den beinahe unbeschränkten Möglichkeiten moderner Mobiltelefone, nicht zuletzt mit ihrer enormen Speicherkapazität. Der Begriff Telefon sei irreführend, „man könne sie auch Videokameras nennen oder Adressbücher, Kalender, Aufnahmegeräte, Büchereien, Tagebücher, Fotoalben, Fernseher, Landkarten oder Zeitungen". Sie enthielten „eine digitale Aufzeichnung von beinahe jedem Aspekt des täglichen Lebens, vom Banalen bis zum Intimen". 90% der US-AmerikanerInnen seien im Besitz eines Mobiltelefons. Drei Viertel aller Smartphone-Besitzenden erklärten, sich meist in unmittelbarer Nähe ihrer Geräte aufzuhalten. Und 12% räumten ein, ihr Telefon sogar in der Dusche zu nutzen.

Eine Grundlage des Urteils ist der Fall „Riley v. California". Im Jahr 2009 hatte die Polizei in San Diego den Autofahrer David Riley angehalten, weil sein Nummernschild abgelaufen war. In seinem Kofferraum fanden dann die Beamten Waffen. Diese werteten daraufhin, ohne ein Gericht um Erlaubnis zu fragen, sein Mobiltelefon aus, fanden Hinweise auf eine Gang und eine frühere Schießerei. Letztlich wurde Riley von der Justiz in Kalifornien wegen versuchten Mordes zu 15 Jahren Haft verurteilt. Das Gericht fordert nun von der Polizei, sich vor der Auswertung einen Durchsuchungsbefehl zu besorgen. „Dass es die Technik jedem Einzelnen nun erlaubt, all diese Informationen bei sich zu haben, macht diese Informationen nicht weniger schützenswert." Der vorsitzende Richter erinnerte an die treibenden Kräfte der US-amerikanischen Revolution gegen die britischen Kolonialherren. Eine davon war die Abscheu vor „allgemeinen Ermächtigungen", die es britischen Offizieren erlaubten, ohne jeden Anfangsverdacht in Häuser einzudringen und nach Beweisen für kriminelles Handeln zu suchen.

Das Urteil betrifft ausdrücklich das Vorgehen der Polizei. Die millionenfache und weltweite Handy-Überwachung durch den US-Geheimdienst National Security Agency (NSA) wurde darin nicht erwähnt. Eine Fußnote im Urteilstext deutet jedoch an, dass sich der Supreme Court dazu ein separates Grundsatzurteil vorbehält. Präsident Barack Obama hatte nach dem Bekanntwerden der NSA-Überwachung eine Reform verordnet. Diese sieht vor, dass die NSA künftig Handy-Daten nicht mehr selbst speichern dürfe. Dies sollten vielmehr private Telefongesellschaften übernehmen. Die NSA könne die Gespräche nach einer Genehmigung des zuständigen Geheimgerichts einsehen (Richter, Fast schon ein Körperteil, SZ 27.06.2014, 2; Richter, Der Schlüssel zu allem, SZ 28./29.06.2014, 4; Höchstes US-Gericht beschränkt Durchsuchung von Handys www.heise.de 26.06.2014, http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf).

EuGH

EU-Rat zu Transparenz bei SWIFT-Verhandlungen verpflichtet

Europas Regierungen müssen gemäß einem Urteil der ersten Kammer des Europäischen Gerichtshofes (EuGH) vom 03.07.2014 in internationalen Verhandlungen transparenter werden (C-350/12 P). Der Rat der Europäischen Union (EU) unterlag damit im Berufungsverfahren gegen ein entsprechendes Urteil des erstinstanzlichen Gerichts der Europäischen Union (EG). Die Luxemburger Richter bestätigten zwar die Schutzwürdigkeit der Verhandlungsstrategie in den EU-US-Verhandlungen

zum Bankdatentransfers (SWIFT, später Terrorist Finance Tracking Programm, TFTP), doch rechtfertige ein lediglich „hypothetisches Risiko“ die Geheimhaltung von Dokumenten nicht. Der Rat müsse ausführlich darlegen, inwieweit das öffentliche Interesse „konkret und tatsächlich“ in Gefahr ist. Im Falle der Stellungnahme von Ratsjuristen zu den Rechtsgrundlagen der Verhandlungen überwiege das Recht der Öffentlichkeit auf Einsicht.

Die niederländische EU-Abgeordnete Sophia In‘t Veld hatte bereits 2009 geklagt, weil der EU-Rat ihr Ersuchen auf Einsicht in die Stellungnahme der Ratsjuristen zur Rechtsgrundlage der SWIFT-Geheimverhandlungen rundweg ablehnte. Das nach Bekanntwerden des unkontrollierten Zugriffs der US-Behörden auf die Bankdaten aller EU-BürgerInnen ausgehandelte SWIFT-Abkommen war erst im zweiten Anlauf als Kontrollmechanismen eingefügt worden und vom EU-Parlament angenommen worden. In‘t Veld hatte die Auffassung vertreten, dass die Offenlegung des Ratsgutachtens ein anderes Licht auf die Verhandlungen mit den USA hätte werfen können und erstritt vor dem EG einen Teilerfolg.

Das EG meinte, dass Verfahrenstransparenz den Organen der Gemeinschaft in den Augen der Öffentlichkeit mehr Legitimität verleihe und eine öffentliche Diskussion ermögliche. Informationen vorzuenthalten nähre dagegen Zweifel an der Rechtmäßigkeit des Rechtsakts und der Legitimität des Entscheidungsprozesses selbst. Weil das Gericht eine Geheimhaltung von Verhandlungspositionen selbst durchaus bejahte, trug es dem Rat auf, erneut zu prüfen, welche Teile der Ratsdokumente der klagenden Abgeordneten zur Verfügung gestellt werden könnten. Der EU-Rat wollte überhaupt keine Transparenz und legte Berufung beim EuGH mit der Begründung ein, die Wahl der Rechtsgrundlage und möglicher Streit darüber könne die Verhandlungsposition der EU unterminieren und vom Verhandlungspartner ausgenutzt werden. Auch das Parlament könne versuchen, den laufenden Verhandlungsprozess zu beeinflussen. Das Gericht müsse die in der Transparenzverordnung (EG 1049/2001) vorgesehenen Ausnahmen vom Recht auf Zugang zu Dokumenten streng auslegen.

Der EuGH wies die Berufung des Rates in allen Punkten zurück. Der Rat sei den Nachweis schuldig geblieben, warum öffentliche Interessen durch die Veröffentlichung der Stellungnahme zur Rechtsgrundlage gefährdet seien. Ein bloßer Verweis reiche nicht aus, insbesondere, wenn er gleich zwei verschiedene im Gesetz vorgesehene Ausnahmen vom Zugangsrecht anführt. In‘t Veld begrüßte das Urteil. Die wieder im Mai 2014 ins EU-Parlament gewählte Abgeordnete forderte dringend Verbesserungen in den Transparenz-Gesetzen der Gemeinschaft. Ein sich über fünf Jahre hin ziehendes Gerichtsverfahren sei zu aufwändig und zu teuer für die Bürger. Sie hatte auch erfolglos auf Zugang zu ACTA-Dokumenten geklagt und betreibt mehrere weitere Verfahren vor dem Ombudsmann der EU, unter anderem wegen eines geheim gehaltenen Europol-Prüfberichts zu den laufenden Bankdatentransfers. Das SWIFT/TFTP-Abkommen ist seit den Enthüllungen Snowdens wieder in der Kritik. Angesichts der Informationen über das durch US-Dienste abgehörte EU-Büro wirkt die im Verfahren hoch gehaltene Notwendigkeit, Verhandlungsstrategien vor den „Partnern“ geheim zu halten, etwas beschädigt (Ermert, Geheimverhandlungen: Europas Regierungen müssen etwas transparenter werden, www.heise.de 04.07.2014; Urteil für mehr Transparenz, SZ 04.07.2014, 7).

Irish High Court

EuGH-Vorlage wegen Safe-Harbor bei Facebook

In einer von dem Wiener Juristen Max Schrems angestoßenen Klage gegen die Untätigkeit des Irischen Datenschutzbeauftragten wegen der Datenübermittlung von Facebook Ireland Ltd. zur Konzernmutter Facebook Inc. in den USA entschied der irische High Court in Dublin mit Beschluss vom 18.06.2014, dem Europäischen Gerichtshof (EuGH) die Frage nach der Verbindlichkeit des Safe-Harbor-Beschlusses der EU-Kommission aus dem Jahr 2000 vorzulegen. Der Kläger machte geltend, dass er durch die Massendatenabfrage des US-amerikanischen Geheimdienstes National Security Agency (NSA) bei der Facebook Inc. in den USA als Facebook-Mitglied in seinen Datenschutzrechten verletzt sei. Eine entsprechende Aufforderung zum Tätigwerden wies der Irische Datenschutzbeauftragte zurück.

Der High Court stellte fest, dass die Erwartung von Schrems an die Datenschutzbehörde keineswegs „ungerechtfertigt oder schikanös“ (frivolous or vexatious) sei. Es könne von dem Kläger nicht verlangt werden, dass er einen Datenmissbrauch in den USA nachweist. Für ein Tätigwerden der Aufsichtsbehörde genüge die begründete Befürchtung, Opfer US-amerikanischer Sicherheitsbehörden zu sein, wenn diese routinemäßig und pauschal massenhaft Personendaten erfassen, wie dies gemäß den Enthüllungen von Edward Snowden der Fall ist. Das Gericht bestätigte, dass nach irischem Recht eine Übermittlung von Personendaten in ein Land verboten ist, das keinen hinreichenden Datenschutz- und Grundrechtsstandard aufweist. Dieser verfassungsrechtlich begründete Schutz würde verletzt, wenn staatliche Behörden massenhaft und undifferenziert von zu Hause aus initiierte Kommunikation überwacht, ohne dass es hierfür hinreichende objektive Gründe der Kriminalitätsbekämpfung und der inneren Sicherheit und angemessene und überprüfbare rechtliche Schutzmaßnahmen gäbe.

Der Kläger wirft dem sozialen Netzwerk vor, die Daten von Millionen seiner europäischen Nutzer an die USA zu übermitteln. Personenbezogene Daten dürften aber nur in ein anderes Land weitergegeben werden, wenn dort angemessener Datenschutz gewährleistet wird. Dieses Prinzip sehen die Studierenden von „Europe versus Facebook“ nach den Enthüllungen über die Spionage der NSA infrage gestellt. Die irische Behörde entschied aber, nicht für die Prüfung von EU-Verträgen zuständig zu sein. Facebook und andere betroffene Unternehmen erklären, sie gäben Nutzerdaten nur auf spezielle Anfragen und keinesfalls massenhaft direkt an US-Behörden weiter. In Enthüllungen des Aufdeckers Edward Snowden über das NSA-Programm “Prism” heißt es jedoch, der Geheimdienst habe weitreichenden Zugriff auf die Server von Internetdiensten wie Facebook.

Der High Court wandte sich an den EuGH, weil er meint, dass der Irische Datenschutzbeauftragte durch den Safe-Harbor-Beschluss der EU-Kommission aus dem Jahr 2000 gebunden sein könnte, der wegen der Safe-Harbor-Zertifizierung von Facebook annahm, dass dort ein für die Datenübermittlung hinreichender Datenschutzstandard besteht. Die Frage des Gerichts an den EuGH geht dahin, ob eine Datenschutzaufsichtsbehörde bei ihrer datenschutzrechtlichen Beurteilung der Übermittlung in ein drittes Land, hier die USA, an die Regelungen der europäischen Datenschutzrichtlinie aus dem Jahr 1995 und den Beschluss der EU-Kommission zu Safe Harbor aus dem Jahr 2000 im Hinblick auf die 2009 in Kraft getretene Europäische Grundrechte-Charta gebunden ist, die in den Art. 7 und 8 die Privatsphäre und den Datenschutz gewährleistet. Weiter stellt das Gericht die Frage, wenn Safe Harbor nicht verbindlich ist, ob eine Datenschutzaufsichtsbehörde Ermittlungen angesichts der faktischen Entwicklungen seit der Kommissionsentscheidung im Jahr 2000 durchführen kann (Randnummer 71 der Entscheidung).

Die Gruppe um Schrems „Europe versus Facebook“ geht seit längerer Zeit in Irland gegen den US-Internetkonzern rechtlich vor, der dort seinen europäischen Firmensitz hat. Zuletzt legte Schrems 2013 Beschwerde gegen die irische Datenschutzbehörde ein, da diese sich geweigert hatte, die Vorwürfe des österreichischen Juristen zu prüfen. Schrems begrüßte die irische Gerichtsentscheidung. „Es ist offensichtlich, dass Facebook Ireland nicht befugt sein kann, bei Grundrechtsverletzungen die US-Regierung zu unterstützen, wenn selbst unsere eigene Regierung zu derartigen Maßnahmen nicht befugt ist.“ Schrems nimmt insofern Bezug auf die Entscheidung des EuGH zur Vorratsdatenspeicherung, die eine Massenüberwachung verbietet. „Wir waren nicht auf einen direkten Verweis an den EuGH vorbereitet, aber das ist das beste Ergebnis, das wir uns hätten wünschen können. Wir werden nun das Urteil im Detail studieren und sobald als möglich den nächsten Schritt machen.“

Die deutschen Datenschutzbehörden hatten schon mit Beschluss des Düsseldorfer Kreises vom 28./29.04.2010, also vor den Snowden-Enthüllungen, festgestellt, dass allein die formale Zertifizierung als Safe-Harbor-Unternehmen eine Übermittlung nicht rechtfertigt. Mit den Snowden-Erkenntnissen dürfte endgültig klar sein, dass z. B. bei Facebook kein hinreichender Grundrechtsschutz nach europäischem Verständnis gewährleistet ist. Inzwischen wurde selbst von der EU-Kommission die Ansicht vertreten, dass die Geschäftsgrundlage von Safe Harbor weggefallen ist. Mit der Vorlagefrage kann der EuGH verbindlich feststellen, dass dies zutrifft.

Der Leiter des Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) Thilo Weichert kommentiert die EuGH-Vorlage durch den irischen High Court: „Die angestrengte Rechtsklärung ist sehr zu begrüßen. Es ist zu hoffen, dass der EuGH in Fortführung seiner bisherigen Rechtsprechung klarstellt, dass Safe Harbor nicht (mehr) verbindlich ist. Politisch und rechtlich noch besser wäre es, wenn die EU-Kommission angesichts der NSA-Überwachung Safe Harbor offiziell aufheben würde“ (Europe v. Facebook, www.europe-v-facebook.org/hcj.pdf; ULD, ULD begrüßt Safe-Harbor-Vorlage wegen Facebook beim EuGH, www.datenschutzzentrum.de 20.06.2014).

BVerfG

Ärztepranger bei Falschabrechnung zulässig

Mit Beschluss vom 03.03.2014 bestätigte das Bundesverfassungsgericht (BVerfG), dass eine berufsgerichtliche Entscheidung, mit der besonders schwerwiegende berufsrechtliche Verfehlungen sanktioniert werden, auf entsprechender gesetzlicher Grundlage kraft richterlicher Anordnung auch nichtanonymisiert im Ärzteblatt veröffentlicht werden darf (1 BvR 1128/13). Die maßgebliche Vorschrift des nordrhein-westfälischen Heilberufsgesetzes (HeilBerG NRW) enthalte eine verfassungskonforme Rechtsgrundlage für die Urteilsveröffentlichung; die Berufsgerichte hätten sie im konkreten Fall nach verfassungsrechtlichen Maßstäben zutreffend angewendet.

Dem Beschwerdeführer, einem niedergelassenen Facharzt, hatte die Ärztekammer vorgeworfen, gegenüber Privatpatienten überhöhte Rechnungen erstellt zu haben. Den Begriff der „Sitzung“ im Sinne der Gebührenordnung habe der Beschwerdeführer zu seinem Vorteil dahingehend ausgelegt, dass Sitzungen auch an Tagen stattgefunden hätten, an denen die Patienten nicht in der Praxis waren. Für das Berufsgericht für Heilberufe war dies ein Verstoß gegen seine Berufspflichten. Es erkannte auf die Entziehung des passiven Berufswahlrechts sowie auf eine Geldbuße in Höhe von 25.000 Euro und ordnete zudem an, dass die Ärztekammer nach § 60 Abs. 3 HeilBerG NRW berechtigt sei, das Urteil nach Rechtskraft im Ärzteblatt der zuständigen Ärztekammer zu veröffentlichen. Nach dieser Vorschrift kann „in besonderen Fällen ... auf Veröffentlichung der Entscheidung erkannt werden“. Das Landesberufsgericht für Heilberufe reduzierte die Geldbuße auf 20.000 Euro und bestätigte die weiteren Sanktionen. Die Verfassungsbeschwerde wendet sich gegen diese beiden Entscheidungen sowie mittelbar gegen § 60 HeilBerG NRW.

Das BVerfG wies die Beschwerde zurück und bestätigte, dass die Regelungen des HeilBerG hinreichend bestimmt sind. Aus der Tatsache, dass zu dem hier relevanten Tatbestandsmerkmal der „Sitzung“ unterschiedliche Auffassungen vertreten werden, könne nicht gefolgert werden, dass deshalb die der berufsrechtlichen Sanktion zugrunde liegenden Regelungen nicht bestimmt genug seien, um eine berufsgerichtliche Verurteilung zu rechtfertigen. Das BVerfG bestätigte auch die Vereinbarkeit der angegriffenen Entscheidungen mit dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Eine Regelung, die zu Eingriffen in das allgemeine Persönlichkeitsrecht ermächtigt, sei nur zulässig, wenn sie zum Schutz eines gewichtigen Gemeinschaftsgutes geeignet und erforderlich ist und der Schutzzweck hinreichend schwer wiegt, so dass er die Beeinträchtigung des Persönlichkeitsrechts in ihrem Ausmaß rechtfertigt. § 60 Abs. 3 HeilBerG NRW genüge diesen Anforderungen; die Regelung sei insbesondere verhältnismäßig. Sie betrifft Angehörige der Heilberufe,

denen ein besonderes, schützenswertes Vertrauen entgegengebracht wird. Das Berufsrecht kann Fehlverhalten, das dieses Vertrauen erschüttert oder zu erschüttern geeignet ist, mit geeigneten Maßnahmen sanktionieren. Zulässig sei danach auch die nichtanonymisierte Veröffentlichung einer rechtskräftigen berufsgerichtlichen Verurteilung. Eine solche Maßnahme finde ihre Rechtfertigung in einem berechtigten Interesse an einer Information der Allgemeinheit, insbesondere der Gemeinschaft der Versicherten wie auch der Kammerangehörigen, die sodann ihr Verhalten nach Kenntnis einer solchen Verfehlung steuern können. Neben dieser im Grundsatz generalpräventiven Wirkung diene die Veröffentlichung auch der weiteren Sanktionierung eines beträchtlichen individuellen Fehlverhaltens, das auch die Gefahr einer höheren Kostenlast für die Gemeinschaft der Versicherten in sich trägt. Eine personifizierte Veröffentlichung sei jedenfalls dann verfassungsrechtlich unbedenklich, wenn es sich um vereinzelte, herausgehobene Fälle handelt. Die Verhältnismäßigkeit werde gewahrt, sofern die Veröffentlichung nur in einem berufsrechtlichen Medium und einmalig erfolgt. Das BVerfG akzeptierte im konkreten Fall auch, dass die Berufsgerichte das dem Beschwerdeführer vorgeworfene Berufsvergehen als besonders schwerwiegend eingeordnet haben, weil in einer systematischen Vorgehensweise mit dem Ziel eines den Vorschriften der Gebührenordnung widersprechenden Abrechnungssystems eine hohe Schadensneigung begründet liege (Erfolglose Verfassungsbeschwerde gegen die Veröffentlichung eines berufsgerichtlichen Urteils, PM BVerfG Nr. 31/2014 02.04.2014).

BGH

Nutzer-Datenherausgabe durch Bewertungsportale nur mit Erlaubnis

Der Bundesgerichtshof (BGH) hat mit Urteil vom 01.07.2014 entschieden, dass ein Betroffener keinen Anspruch gegen einen Internetportalbetreiber auf Herausgabe der Anmeldedaten von einem Benutzer hat, der über den Betroffenen falsche Informationen ins Netz gestellt hat (Az. VI ZR 345/13). Dies entschied der Bundesgerichtshof im Falle eines Arztes, der von einen Bewertungsportal für Ärzte Auskunft über einen Nutzer verlangte, der mehrfach falsche Behauptungen über ihn aufgestellt hatte. Der frei praktizierende Arzt machte einen Auskunftsanspruch gegen die Beklagte, die Betreiberin des Internetportals Sanego ist, das Bewertungen von Ärzten ermöglicht, geltend. Im November 2011 hatte er auf der Internetseite der Beklagten eine Bewertung entdeckt, in der über ihn verschiedene unwahre Behauptungen aufgestellt wurden. Im Juni 2012 wurden weitere, den Kläger betreffende Bewertungen mit unwahren Tatsachenbehauptungen veröffentlicht. Auf sein Verlangen hin wurden die Bewertungen jeweils von der Beklagten gelöscht. Am 04.07.2012 erschien (jedenfalls) bis November 2012 erneut eine Bewertung mit den von dem Kläger bereits beanstandeten Inhalten.

Das Landgericht hat die Beklagte zur Unterlassung der Verbreitung der vom Kläger beanstandeten Behauptungen und zur Auskunft über Name und Anschrift des Verfassers der Bewertung vom 04.07.2012 verurteilt. Die dagegen gerichtete Berufung der Beklagten hatte keinen Erfolg. Das Oberlandesgericht (OLG) hat einen Auskunftsanspruch des Klägers gegen die Beklagte wegen der bei ihr hinterlegten Anmeldedaten des Verletzers gemäß §§ 242, 259, 260 BGB bejaht. § 13 Abs. 6 Satz 1 Telemediengesetz (TMG), wonach ein Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist, schließe den allgemeinen Auskunftsanspruch nicht aus.

Mit der vom OLG beschränkt auf den Auskunftsanspruch zugelassenen Revision verfolgte die Beklagte erfolgreich ihren Antrag auf Abweisung der Klage weiter. Der BGH wies die Klage auf Auskunftserteilung ab. Der Betreiber eines Internetportals ist danach in Ermangelung einer gesetzlichen Ermächtigungsgrundlage im Sinne des § 12 Abs. 2 TMG grundsätzlich nicht befugt, ohne Einwilligung des Nutzers dessen personenbezogene Daten zur Erfüllung eines Auskunftsanspruchs wegen einer Persönlichkeitsrechtsverletzung an den Betroffenen zu übermitteln. Nach dem Gebot der engen Zweckbindung des § 12 Abs. 2 TMG dürften für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwendet werden, soweit eine Rechtsvorschrift dies erlaubt oder der Nutzer – was hier nicht in Rede stand – eingewilligt hat. Ein Verwenden im Sinne des § 12 Abs. 2 TMG stelle auch eine Übermittlung an Dritte dar. Eine Erlaubnis durch Rechtsvorschrift kommt außerhalb des TMG nach dem Gesetzeswortlaut lediglich in Betracht, wenn sich eine solche Vorschrift ausdrücklich auf Telemedien bezieht. Eine solche Vorschrift habe der Gesetzgeber bisher – bewusst – nicht geschaffen.

Dem durch persönlichkeitsrechtsverletzende Inhalte einer Internetseite Betroffenen kann allerdings ein Unterlassungsanspruch gegen den Diensteanbieter zustehen (BGH U. v. 25.10.2011 – VI ZR 93/10, BGHZ 191, 219), den das OLG im Streitfall auch bejaht hat. Darüber hinaus darf der Diensteanbieter nach § 14 Abs. 2, § 15 Abs. 5 Satz 4 TMG auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestands-, Nutzungs- und Abrechnungsdaten erteilen, soweit dies u. a. für Zwecke der Strafverfolgung erforderlich ist.

Thomas Spaeing, Vorstandsvorsitzender des Bundesverbands der Datenschutzbeauftragten Deutschlands (BvD), wies darauf hin, dass das hier zum Tragen kommende Datenschutzprinzip den Datenschutz nicht zum Täterschutz macht. Im Falle eines Straftatverdachts bestünden für Ermittlungsbehörden verschiedene gesetzliche Befugnisse, Daten zur Verfolgung von Straftaten zu erlangen (BvD e. V., Bundesgerichtshof stärkt Datenschutzprinzip: Datenherausgabe bei Bewertungsportalen nur mit Erlaubnis, PE v. 02.07.2014; BGH, Kein Anspruch auf Auskunft über Anmeldedaten gegen den Betreiber eines Internetportals, PE 01.07.2014).

LG Berlin

Whatsapp-AGB bitte in Deutsch!

Das US-Unternehmen Whatsapp, das kürzlich von Facebook aufgekauft wur-

de, wurde mit Versäumnisurteil vom 09.05.2014 des Landgerichts (LG) Berlin verurteilt, den Impressumspflichten nach dem Telemediengesetz (TMG) nachzukommen und die Allgemeinen Geschäftsbedingungen (AGB) für seine Messenger-App auf Deutsch anzubieten (Az. 15 O 44/13). Die ansonsten deutschsprachige Website gibt die AGB nur in englischer Sprache wider. Geklagt hatte der Bundesverband der Verbraucherzentralen (vzbv), nachdem er Whatsapp bereits im Jahr 2012 aus denselben Gründen zweimal erfolglos abgemahnt hatte:

„1. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise Ordnungshaft bis zu sechs Monaten oder Ordnungshaft bis zu sechs Monaten, diese zu vollstrecken an dem Chief Executive Officer, zu unterlassen,

a. *im Rahmen geschäftlicher Handlungen auf der Webseite www.whatsapp.com*
- *den Vertretungsberechtigten der Beklagten*
- *die geographische Anschrift, unter der die Beklagte niedergelassen ist,*
- *einen zweiten Kommunikationsweg neben der E-Mail-Adresse,*
- *das öffentliche Register, in das die Beklagte eingetragen ist, sowie die in diesem Register verwendete Kennung nicht leicht, unmittelbar und ständig verfügbar zu machen*

und/oder

b. *im Rahmen geschäftlicher Handlungen gegenüber Verbrauchern in Deutschland Produkte und Dienstleistungen unter http://www.whatsapp.com anzubieten und hierbei Allgemeine Geschäftsbedingungen zu verwenden, die nicht in deutsche Sprache verfügbar sind. …*

Der Kläger ist der Dachverband unter anderem der deutschen Verbraucherzentralen und in die Liste nach § 4 Unterlassungsklagegesetz (UKlaG) eingetragen. Die Beklagte betreibt die Webseite www.whatsapp.com und bietet dort auch für Verbraucher in Deutschland ein Kommunikationsprogramm an. Die Webseite ist, wenn sie von Deutschland aus aufgerufen wird, fast ausschließlich in deutsche Sprache abgefasst. Die Beklagte hält die in dem Urteilstenor zu 1. genannten Informationen auf ihrer Webseite nicht bereit. Allgemeine Geschäftsbedingungen bietet sie dort nur in englischer Sprache an. Auf entsprechende Abmahnungen des Klägers vom 19. Juli 2012 und 9. Oktober 2012 hat die Beklagte nicht reagiert.

Das Gericht hat die Klage nebst Übersetzung förmlich am Sitz der Beklagten zustellen lassen mit dem Ergebnis, dass dort am 23. Juli 2013 die Entgegennahme amtlicher Dokumente verweigert wurde. …

Die Klage ist zulässig und begründet. Es war durch Versäumnisurteil im schriftlichen Vorverfahren zu entscheiden, § 331 Abs. 3 ZPO. Die Klage gilt als am 23. Juli 2013 wirksam zugestellt. Die Beklagte konnte dies nicht dadurch vereiteln, dass sie sich geweigert hat, die ihr damals angebotene förmliche Zustellung entgegenzunehmen.

Der Kläger kann nach §§ 8 Abs. 1 und Abs. 3 Nr. 3, 4 Nr. 11 des Gesetzes gegen den unlauteren Wettbewerb (UWG) verlangen, dass die Beklagte die hier nach § 5 Abs. 1 Nr. 1, Nr. 2 und Nr. 4 Telemediengesetz (TMG) vorgeschriebenen Informationspflichten erfüllt und ihre unzureichende Anbieterkennzeichnung ergänzt.

Nach §§ 3 Abs. 1 Nr. 1, 4 Abs. 1, 2 UKlaG hat der Kläger ferner einen Anspruch darauf, dass die Beklagte es unterlässt, deutschen Verbrauchern ihre Allgemeinen Geschäftsbedingungen (AGB) nur in englischer Sprache anzubieten. Nach § 305 Abs. 2 Bürgerliches Gesetzbuch (BGB) müssen AGB von den Verbrauchern in zumutbarer Weise zur Kenntnis genommen werden können. Das ist nicht gewährleistet, wenn Verbraucher in Deutschland, die von dem Anbieter im Übrigen in deutscher Sprache angesprochen werden und von denen – wie hier – nicht überwiegend erwartet werden kann, dass sie AGB in englischer (Rechts-)Sprache ohne Weiteres verstehen, die AGB nur in englischer Sprache aufrufen können (vergleiche AG Köln – 114 C 22/12 -, Urteil vom 24. September 2012).

Die Verstöße begründen eine Wiederholungsgefahr. Deren Beseitigung ist nicht erkennbar."

Das Urteil ist nicht rechtskräftig. Die AGB oder besser „Terms of Service" von Whatsapp waren kurz nach dem Urteil noch aus einem anderen Grund Thema in den deutschen Medien: Stein des Anstoßes war Abschnitt 5B, wo sich das Unternehmen das Recht einräumt, Texte und Bilder weltweit und kostenfrei nutzen zu können – und zwar auch in veränderter Form und etwa zu Werbezwecken (vzbv, http://www.vzbv.de/cps/rde/xbcr/vzbv/WhatsApp-LG-Berlin-15_0_44_13.pdf; Urteil: Whatsapp muss deutsche AGB bereitstellen, www.heise.de 27.05.2014).

LG Koblenz

Fitnessclub-AGB zu Videoberwachung unzulässig

Gemäß einem Urteil des Landgerichts (LG) Koblenz vom 19.12.2013 muss bei der Kameraüberwachung in einem Fitnessclub der Zweck und der Umfang der Überwachung und der Speicherung der Aufnahmen hinreichend deutlich in den AGB konkretisiert sein (Az. 3 O 205/13). Ist dies nicht der Fall, liegt eine unangemessene Benachteiligung der KundInnen und somit eine unzulässige Kameraüberwachung vor. Ein Verbraucherschutzverein klagte gegen den Fitnessclub auf Unterlassung der Verwendung mehrerer Klauseln in den AGB: „[Im Fitnessclub] werden zur Erhöhung der Sicherheit Teilbereiche durch Videokameras überwacht. Einzelfallbezogen werden Aufnahmen gespeichert, soweit und solange dies zur Sicherheit der Mitglieder und zur Aufklärung von Straftaten notwendig ist. … Das Mitglied stimmt einer dauerhaften Kameraüberwachung durch [den Fitnessclub] zur Sicherheitserhöhung zu." Der Verbraucherschutzverein hielt die Klauseln für mit dem Bundesdatenschutzgesetz (BDSG) nicht vereinbar und zudem für intransparent.

Das LG Koblenz gestand dem Verbraucherschutzverein einen Anspruch auf Unterlassung zu. Die Klauseln haben die Kunden unangemessen benachteiligt (§ 307 Abs. 1 Satz 2 Bürgerliches Gesetzbuch – BGB), da sie weder klar noch verständlich bzw. mit dem wesentlichen Grundgedanken der §§ 626, 314 BGB vereinbar gewesen seien. Durch die Formulierung „Überwachung von Teilbereichen" sei nicht hinreichend konkretisiert, welche Bereiche kamera-

überwacht wurden. Die Formulierung deute auf einen Beurteilungsspielraum hin, was unter Umständen zu einem ungerechtfertigten Eingriff in das Persönlichkeitsrecht der Mitglieder hätte führen können. Zudem sei auch der Zweck und der Umfang der Speicherung der Daten nicht ausreichend konkretisiert worden. Es hätte daher zu einer Speicherung kommen können, die über das erforderliche Maß hinausgegangen wäre (Kameraüberwachung im Fitnessclub: Zweck und Umfang der Überwachung und Speicherung der Aufnahmen müssen ausreichend in den AGB konkretisiert sein, www.kostenlose-urteile.de 15.01.2014; SZ 11.06.2014, 21).

VG Hannover

Demo-Filmen nur bei konkreter Gefahr

Das Verwaltungsgericht (VG) Hannover hat mit Urteil vom 14.07.2014 der Polizei enge Grenzen für den Einsatz von Kameras bei Demonstrationen gesetzt (10 A 226/13). Wenn die Polizei vorsorglich einen Kamerawagen mit einer bereits ausgefahrenen Mastkamera bereithalte, führe alleine schon das Gefühl des Beobachtetwerdens zu einer Einschränkung der Versammlungsfreiheit. Das Gericht gab der Klage von Teilnehmenden einer Kundgebung gegen Neonazis statt, die sich von dem Wagen mit der Kamera abgeschreckt gefühlt hatten. Diese Art der Vorbereitung auf ein alleine bei Ausschreitungen zulässiges Filmen gehe zu weit. Die innere Einstellung der Demonstrationsteilnehmenden werde dadurch berührt, vor allem weil sie aus einiger Entfernung überhaupt nicht erkennen könnten, ob die Kamera laufe oder nicht. Das Grundrecht der Versammlungsfreiheit wiege so schwer, dass die Polizei im Ernstfall die geringe Verzögerung in Kauf nehmen müsse, die sich durch das Ausfahren der Kamera ergebe.

Teilnehmende der Demonstration gegen Rechts Anfang 2012 in Bückeburg hatten von der Polizei verlangt, die aus ihrer Sicht rechtswidrigen Aufnahmen von der Demonstration zu löschen. Wegen der ausgefahrenen Kamera waren sie davon ausgegangen, auch gefilmt worden zu sein. Die Polizei jedoch erklärte, keine Aufnahmen gemacht zu haben. Sie hielt das Bereithalten des Kamerawagens für notwendig, um ihre gesetzlichen Aufgaben zu erfüllen. Das Gericht entschied, das Bereithalten der ausgefahrenen Kamera wäre nur dann zur Gefahrenabwehr erforderlich und gerechtfertigt gewesen, wenn eine unfriedliche Wendung der Demonstration konkret bevorgestanden hätte.

Nach dem niedersächsischen Versammlungsgesetz darf die Polizei einzelne Personen, aber auch die gesamte Kundgebung im Überblick filmen, um eine von den Demonstrierenden ausgehende Gefahr für die öffentliche Sicherheit abzuwehren. Eine unübersichtliche Versammlung darf auch mit Kameras beobachtet werden, wenn die öffentliche Sicherheit und Ordnung in Gefahr sind. Bei friedlichen Demos sind Kameras tabu.

Nach dem niedersächsischen Versammlungsgesetz (§ 12) darf die Polizei „zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit“ Einzelpersonen oder auch in der Übersicht die gesamte Kundgebung filmen oder fotografieren. Wenn friedfertige Teilnehmende dabei unvermeidlich mit auf die Aufzeichnung gelangen, ist dies erlaubt. Im Anschluss müssen die Aufzeichnungen gelöscht oder anonymisiert werden, wenn sie nicht zur Verfolgung von Straftaten oder als Beweis benötigt werden.

Auf der anderen Seite ist das Filmen und Fotografieren mehrerer oder einzelner Polizeibeamter nach dem Kunsturhebergesetz (KUG) im Allgemeinen unzulässig. Im Einzelfall ist aber abzuwägen, ob der Polizist im Einsatz als „relative Person der Zeitgeschichte“ Foto- und Filmaufnahmen dulden muss, oder sein Recht am eigenen Bild (dieses Recht besitzt jeder Mensch) schwerer wiegt (§§ 22, 23 KUG). Dies ist vor allem der Fall, wenn das Foto Porträtcharakter hat und der Bezug zu dem entsprechenden Ereignis nicht mehr erkennbar ist. Ein Sicherstellen von Kamera und Speicherkarte ist nur berechtigt, wenn die Polizei konkrete Anhaltspunkte dafür hat, dass ein Foto eines Beamten veröffentlicht oder verbreitet wird, ohne dass dessen Einwilligung dafür vorliegt oder der Beamte dies dulden muss. In diesem Fall handelt es sich um eine Straftat, die mit bis zu einem Jahr Haft oder Geldstrafe geahndet wird (§ 33 KUG) (Gericht schränkt Einsatz von Polizeikameras ein, www.paz-online.de 14.07.2014).

LG Frankfurt

Kamera-Attrappe erlaubt

Das Landgericht (LG) Frankfurt am Main hat in einem Beschluss vom 11.11.2013 festgestellt, dass es Wohnungseigentümer hinnehmen müssen, wenn ein Mit-Wohnungseigentümer an seinem Balkon eine funktionsuntüchtige Kameraattrappe anbringt (2-13 S 24/13). Dadurch würden keine Rechte Dritter verletzt. Nur konkrete und objektive Beeinträchtigungen könnten dazu führen, dass der Wohnungseigentümer die Kamera wieder abbauen muss. Allein die Befürchtung, bei einer Annäherung an den Balkon gefilmt zu werden, genüge nicht. Mangels funktionierender Kamera sei keine Überwachung möglich und das allgemeine Persönlichkeitsrecht werde nicht verletzt (SZ 01.08.2014, 20).

VG Ansbach

Auto-Dashcams nur eingeschränkt zulässig

Das Verwaltungsgericht (VG) Ansbach erklärte mit Urteil vom 12.08.2014 den Einsatz von Auto-Videokameras unter bestimmten Bedingungen für zulässig. Es dürften damit keine Aufnahmen in der Absicht gemacht werden, sie später ins Internet zu stellen, auf YouTube oder Facebook hochzuladen oder Dritten – etwa der Polizei – zu übermitteln. Im konkreten Fall hob das Gericht das behördliche Verbot des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) wegen eines Formfehlers auf. Wegen der grundsätzlichen Bedeutung wurde Berufung zugelassen.

Mit Dashcams – benannt nach dem englischen Wort „dash“ für Armaturenbrett, auf dem die Kameras häufig montiert sind, wollen sich Autofahrer vor allem bei Unfällen gegen andere Verkehrsteilnehmende absichern. Dem Pro-

zess lag eine Klage eines Autofahrers aus Mittelfranken gegen das BayLDA zugrunde, das dem Mann untersagt hatte, eine Dashcam zur Aufzeichnung von Verkehrsverstößen anderer VerkehrsteilnehmerInnen einzusetzen. Dagegen hatte dieser geklagt. Die Klägeranwältin erklärte, ihr Mandant fühle sich häufig von anderen AutofahrerInnen genötigt, sodass er sich zum Einsatz der Kamera gezwungen gesehen habe, um Beweismittel zu sichern. Sie bestätigte, dass ihr Mandant, selbst ein Anwalt, insgesamt 22 AutofahrerInnen wegen Verkehrsdelikten bei der Polizei angezeigt habe. In fünf Fällen hatte er seine Dashcam-Aufnahmen der Polizei zur Verfügung gestellt. Doch die Beamten waren nicht dankbar, sondern meldeten den Dashcam-Nutzer dem BayLDA. Das Gericht forderte den Mann nun auf, seine Bilder zu löschen.

Der Einsatz von Dashcams ist hierzulande – anders als beispielsweise in Österreich – nicht ausdrücklich untersagt. Erlaubt ist beispielsweise der Einsatz der Mini-Kameras für persönliche Zwecke. Im aktuellen Fall habe der Autofahrer mit seinen Videoaufnahmen aber andere Verkehrsteilnehmer bei der Polizei überführen wollen. Damit habe er, so das VG Ansbach, „den persönlichen oder familiären Bereich verlassen, womit das Bundesdatenschutzgesetz (BDSG) Anwendung findet“. Schließlich ließen sich die mit seiner Dashcam in der Öffentlichkeit gefilmten Personen ohne weiteres identifizieren. Das Gericht wies darauf hin, dass das BDSG „heimliche Aufnahmen unbeteiligter Dritter grundsätzlich nicht zulässt und solche Aufnahmen einen erheblichen Eingriff in das Persönlichkeitsrecht auf informationelle Selbstbestimmung der von den Filmaufnahmen betroffenen Personen darstellen“.

Das VG Ansbach wies die Klage nur wegen eines Formfehlers im Untersagungsbescheid des BayLDA zurück. Im konkret verhandelten Fall sei der Verbotsbescheid möglicherweise nicht ausreichend eindeutig formuliert gewesen. So habe die genaue Marken- und Typen-Bezeichnung der von dem klagenden Autofahrer verwendeten Dashcam gefehlt. Der Autofahrer darf die Kamera weiterhin benutzen, aber nicht, um permanent andere Verkehrsteilnehmende zu überwachen. Unzulässig sei es, wenn die Bilder den privaten Bereich verlassen, etwa wenn sie im Internet veröffentlicht oder der Polizei zur Verfügung gestellt werden. Grundsätzlich seien die Datenschutzinteressen der heimlich Gefilmten höher zu bewerten als das Interesse des Autofahrers an einem Videobeweis im Fall eines Unfalls. Der Kammervorsitzende Alexander Walk meinte, der Gesetzgeber sei in der Pflicht und müsse überprüfen, ob die Datenschutzbestimmungen auf „On-Board-Kameras“ noch passten oder ob das BDSG ergänzt werden müsse.

Das Gericht teilte nicht die Auffassung des Landesamtes, wonach ein Verbot solcher Kameras datenschutzrechtlich in jedem Fall zwingend notwendig sei. Die gesetzlich eingeräumten Ermessensspielräume müssten etwa dann großzügiger ausgelegt werden, wenn es sich bei solchen Aufnahmen eher um Videos von touristischem Interesse handele – „etwa bei einer Ausflugsfahrt durch die Fränkische Schweiz“.

In Österreich droht Autofahrern mit Dashcam an Bord ein saftiges Bußgeld von bis zu 10.000 Euro. Großer Beliebtheit erfreuen sich Dashcams in Russland. Dort sind die aufgezeichneten Filme vor Gericht zugelassen. Im Internet kursieren unzählige Videos, die spektakuläre Unfälle und kuriose Ereignisse zeigen – darunter auch Aufnahmen zu einem Meteoritenregen im Ural im Februar 2013 (Dashcams verstoßen gegen Datenschutzgesetz, www.spiegel.de 12.08.2014; Streit um Dashcams: Teilerfolg für Datenschützer, www.heise.de 12.08.2014; Hildebrand, Spion an der Scheibe, SZ 13.08.2014, 8).

Buchbesprechungen



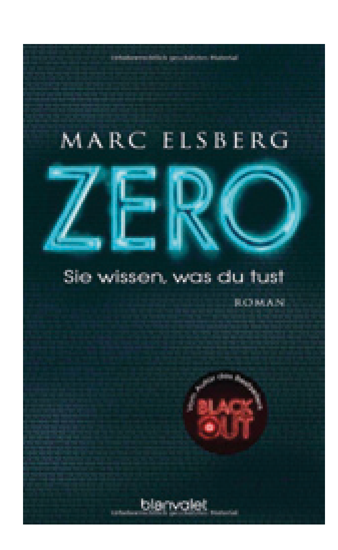
Albrecht, Jan Philip
Finger weg von unseren Daten!
Wie wir entmündigt und ausgenommen werden
Knaur Taschenbuch, München 2014,
191 S. ISBN 978-3-426-78687-1

(TW) Soweit ich das übersehen kann, hatte bisher noch kein deutscher Parlamentarier ein Buch über den Datenschutz geschrieben. Gründe hierfür dürfte es viele geben: mangelndes damit zu erzielendes Renommee, mangelnde Kompetenz, mangelndes Engagement. Diese Mängel gelten alle nicht für den im Mai 2014 erneut ins Europaparlament (EP) gewählten Grünen-Abgeordneten J. P. Albrecht. Der junge Autor, ausgebildeter IT-Rechtler und Berichterstatter für die Europäische Datenschutz-Grundverordnung im EP, legt in Buchform sein Verständnis vom Datenschutz dar und gewinnt dadurch weiter an Profil, zeigt Kompetenz und Engagement.

Sein populär und leicht zu lesendes Büchlein beleuchtet die Situation des Datenschutzes in Europa – und in den USA – grundrechtsorientiert, mit kritischer Distanz zu seinem eigenen Parlament und in realistischer Einschätzung der wirtschaftlichen und politischen Gegebenheiten. Er schildert an vielen aktuellen Beispielen, wie die informationelle Fremdbestimmung und Ausbeutung mit Hilfe einer hoch entwickelten Informationstechnik fortgeschritten sind, die Profitmöglichkeiten bei der Auswertung personenbezogener Daten und wie diese durch Lobbyarbeit verteidigt werden. Er zeigt auf, wie Wirt-

schaft und Sicherheitsbehörden in einer unheiligen Allianz gegen das Grundrecht auf Datenschutz ihre Interessen wahren. Besonders aufschlussreich sind seine Kapitel zur politischen Genese der EU-Grundverordnung sowie zu den Begehrlichkeiten der Sicherheitsbehörden. In Bezug auf die Vorratsdatenspeicherung, die NSA-Affäre und insbesondere ACTA beschreibt er die Wechselwirkungen zwischen kritischer außerparlamentarischer Öffentlichkeit, Parlament und politischen Entscheidungen.

Die Stärke des Buches ist zugleich seine Schwäche: Es ist für die NormalbürgerIn – Anfängerin oder Fortgeschrittene – geschrieben und argumentiert sehr assoziativ, garniert mit vielen Einzelinformationen und Hintergründen. Die dadurch erreicht argumentative Dichte führt zu einem Mangel an systematischem Aufbau, an Quellennachweisen und an weitergehenden Informationen. Dies macht das Buch nur eingeschränkt als Quelle für die ExpertIn nutzbar. Schon ein Stichwortverzeichnis würde insofern sehr weiterhelfen. Doch auch für die ExpertIn ist das Büchlein eine hochinformative und argumentative Fundgrube.



Elsberg, Marc
Zero
Sie wissen, was Du tust
blanvalet Verlag, München 2014
ISBN 978-3-7645-049-2

(TW) Ein neues Literaturgenre scheint am Entstehen zu sein: der gesellschaftskritische IT-Thriller. Dabei handelt es sich um Romane, die ihre Spannung und ihren Unterhaltungswert darauf begründen, dass die technischen, politischen, sozialen, psycholgischen, ökonomischen ... Möglichkeiten unserer modernen Informationsgesellschaft ausgereizt und dramatisierend sowohl in Bezug auf einzelne Personen wie die gesamte Gesellschaft dargestellt werden. Filmerisch wurde das Thema schon oft bearbeitet; der Film „Minority Report“ war ein Höhepunkt. Nach George Orwells frühem „1984“ wurden wir lange Zeit vor allem mit ökonomisch interessierten Darstellungen bombardiert, die vom Sillicon Valley ausgehende informationstechnische Heilsversprechungen verbreiteten. Seit Kurzem hat sich der Wind gedreht. Edward Snowden hat uns Einblicke in die Realität gegeben, die zugleich die literarische Phantasie beflügeln. Während „1984“ noch einen weiten Sprung in die Zukunft macht und als „Science Fiction“ mehr oder weniger prominente Nachfolger fand, knüpfen die modernen IT-Thriller viel mehr an der – technisch fortgeschrittenen – Realität an und denken diese weiter.

Wenn von einem solchen Roman dann eine politische Botschaft ausgeht, die spannend erzählt wird, dann sollte dieser empfohlen werden. Dies trifft auf „Zero“ des österreichischen Autors Marc Elsberg zu. Seine Geschichte spielt in der allernächsten Zukunft, in der es Google und Facebook als Datenkraken noch gibt, aber auch ein neues Unternehmen „FreeMee“, das durch Handlungsempfehlungen auf der Grundlage von umfassenden Datenprofilen und Persönlichkeitsanalysen diese zu erfolgreichen Menschen zu machen verspricht. Außerdem gibt es eine geheim agierende Antiüberwachungsinitiative „Zero“, die mit einer spektakulären Überwachungsaktion des US-Präsidenten diesen und seine Administration ziemlich lächerlich aussehen lässt. Eine der literarischen Botschaften ist es, dass die Überwachungstechnik gegen die Überwacher instrumentalisiert werden kann. Zero wird nun von der US-Administration und den Medien gejagt, unter anderem von der britischen Zeitung „Daily“, bei der die Protagnonistin des Buchs „Cyn“ als Journalistin arbeitet. Diese, noch mit eher vortechnischer Sozialisation, beginnt durch den Tod von nahe stehenden Menschen mit der Recherche zu Zero und dem persönlichkeitsverändernden Dienst FreeMee. Letzterer nutzt die Recherchen zur weiteren Steigerung seiner Nutzerzahlen. Die US-Regierung nutzt sie, um Zero auf die Spur zu kommen. Zum Einsatz kommen dabei durchgängig heute schon im Angebot befindliche Techniken: Videobrille, Gesichtserkennung, Personensuchmaschinen, globales Lifestreaming, predictive Policing, wearable Computing, Personenranking, quantified Self, Big Data, sämtliche Smart-Phone-Funktionalitäten, Fahndung über soziale Netzwerke ...

Im Vordergrund steht das Geschäftsmodell von FreeMee, das für Angehörige der US-Administration wegen der politischen Beeinflussungsmöglichkeiten zum attraktiven Partner wird durch seine informationstechnischen Applikationen der Selbstoptimierung. Die technisch realistische Darstellung wird durch spannende Fiktion immer mehr zugespitzt, ohne dass dabei der Realitätskern verloren geht. Am Ende wird der Komplott von FreeMee mit den IT-Waffen, die FreeMee selbst nutzt, aufgedeckt. Dabei endet der Roman nicht – wie beim Genre-Vorbild „1984“ – in der Stabilisierung der Distopie, sondern offen; er lässt optimistische Lesarten zumindest zu. Eine Qualität des Buches liegt darin, dass es nicht belehrend, sondern beschreibend bleibt und die LeserIn zur BeobachterIn auf verschiedenen Ebenen macht. Die sehr widersprüchlichen Ansichten der Charaktere des Buches sprechen für sich. Was der Autor denkt, lässt sich am ehesten, muss sich aber nicht in den Gedanken und Worten von Cyn widerspiegeln. Die LeserIn kann sich ihren eigenen Reim machen über das Szenario einer informationstechnischen Manipulationsgesellschaft, gegen die es sich – entsprechend Cyn oder Zero – zu kämpfen lohnt, die mehr Realität ist, als viele von uns sich einzugestehen bereit sind.

Eine kleine Kritik zum Schluss: Die wichtigsten Personen des Buches haben leider fast durchgängig Allerwelts-Vor-, -Nach- und -Kurznamen, die man sich zunächst nur schwer merken kann. So muss die LeserIn manchmal ans Ende des Buches blättern, wo die Namen den wichtigsten Rollen tabellarisch zugeordnet werden. Erhellend ist für die weniger eingeweihten LeserInnen ein Glossar, das in die noch

für Viele geheime Welt des modernen informationsgesellschaftlichen Vokabulars einführt. Als Urlaubs- wie als Bettlektüre hervorragend geeignet.



Schrems, Max
Kämpf um Deine Daten
edition a, Wien 2014,
ISBN 978-3-99001-086-0, 221 S.

(TW) Neues Grundsätzliches zum Datenschutz kann man eigentlich nicht mehr schreiben, dachte ich. Alles Wesentliche ist schon gesagt. Was wir jetzt brauchen, ist die Bearbeitung der dauernd neuen technischen und praktischen Fragen und die populäre Verbreitung, um Durck auf die Politik auszuüben. Max Schrems, gerade abgeschlossener 27jähriger Jurist aus Wien, ist beim Verfassen seines Buchs „Kämpf um Deine Daten" gelungen, ein populäres Buch zu schreiben und dabei zugleich Grundsätzliches mitzuteilen. Kurz und knapp, informativ, unterhaltsam, engagiert und auf höchstem Niveau argumentierend beantwortet er die wesentlichen aktuellen Fragen zum Datenschutz.

Seine Gruppe „europa-versus-facebook" fordert seit 2011 den US-amerkanischen Betreiber des weltweit größten sozialen Netzwerkes heraus – und Datenschutz von ihm ein. Schrems hat dabei einiges erreicht – etwa, als er mit seiner Gruppe auf Auskunftsersuchen von Facebook CDs erhielt, die in einem Fall ausgedruckt 1222 Seiten umfasst hätte. Damit konnte er nachweisen, was Facebook alles speichert, dass dazu viele vermeintlich gelöschte Daten gehören, und dass alle späteren Auskunftserteilungen der Plattform unvollständig und damit rechtswidrig waren und sind. Im Juni 2014 machte Schrems von sich reden, als auf seine Klage hin der Irish High Court die Frage der Grundrechtsverträglichkeit des Safe-Harbor-Beschlusses der Europäischen Kommission aus dem Jahr 2000 dem Europäischen Gerichtshof vorlegte (s. Seite 130f). Kurz darauf initiierte er gegen Facebook eine Sammelklage vor einem österreichischen Gericht, der sich schon nach zwei Wochen 25.000 Facebook-Nutzende angeschlossen hatten. Dazwischen setzte sich Schrems medienwirksam über vielfältige Facebook-Beschwerden beim irischen Datenschutzbeauftragten sowie Beschwerden wegen Datenübermittlungen in die USA nach den NSA-Enthüllungen von Edgar Snowden mit weiteren Aufsichtsbehörden auseinander und bewies dabei angesichts der vielen Rückschläge Fachkompetenz und Standvermögen.

Sein Buch erzählt nun nicht die vier Jahre seines Kampfes um seine Daten nach. Die Konflikte von europe-versus-facebook mit Facebook, dem irischen Datenschutzbeauftragten und generell Verantwortlichen in Europa und den USA sind nicht das Thema, sondern der Hintergrund und das Material für die Darstellung. Er befasst sich popuärwissenschaftlich mit der Frage, weshalb wir persönlich und als Gesellschaft heute Datenschutz brauchen. Was macht die moderne Datenverarbeitung mit uns, wer verfolgt welche Interessen und wie werden wir bzw. unsere Daten für welche Zwecke und für wessen Nutzen missbraucht. Dabei erläutert er tiefgreifend die komplexen philosophischen, gesellschaftlichen, juristischen, technischen und ökonomischen Zusammenhänge, so dass wissenschaftlich nicht vorgebildete LaiInnen diese nachvollziehen und verstehen können und zugleich SpezialistInnen mit für sie noch nicht bekannten Fakten und Zusammenhängen konfrontiert werden. Analogien aus der analogen Welt erhöhen die Handgreiflichkeit der digitalen Sachverhalte. Auf seinen vielen Veranstaltungen wurde Schrems mit Argumenten und Vorbehalten konfrontiert, mit denen er sich nun systematisch pointiert und qualifiziert auseinandersetzt: „... aber die Leute stellen ja alles ins Netz! Ihr habt doch zugestimmt! Vertrauen im Netz? Naiv! Du hast doch nichts zu verstecken, oder? Wir haben alles anonymisiert! Das Diktat der Technologie. Datenschutz schadet Wirtschaft und Innovation! ... dann kommt der Terror. Bis Du nicht für uns, bist Du gegen uns!"

Schrems demaskiert die Strategien und die Geschäftsmodelle der Unternehmen, analysiert das Nutzerverhalten sowie die Ohnmacht und die weit verbreitete Untätigkeit der Datenschutzbehörden. Die katastrophale Ausstattung der für die europäischen Hauptniederlassungen vieler US-Firmen zuständigen irischen Datenschutzbehörde wird ebenso dargestellt wie die Strategien, mit denen diese Stelle die Datenschutzrechte der BürgerInnen ignorierte und hinterging. Anschaulich legt er dar, wie die IT-Industrie die VerbraucherInnen für sich gewinnen und in Unwissenheit halten, wie sie mit staatlichen Sicherheitsbehörden zusammenarbeiten und wie so die Nutzerüberwachung perfektioniert wird.

Schrems hat den großen Vorteil, aus eigener Anschauung die Verbrauchermanipulation und den Datenschutz in den USA erlebt zu haben und schildert seine Erfahrungen anschaulich. Die USA erweisen sich als das Europa drohende Zukunfts-Horrorszenario der Überwachung, wenn nicht politisch gegengesteuert wird. Hierfür diskutiert er mögliche Strategien und Instrumente: Aktivitäten der Parlamente, der Justiz und der Verwaltung, zivilrechtliche Maßnahmen, technischer Selbstdatenschutz, Selbstregulierung der Wirtschaft... Es überrascht, dass Schrems die Politik, wie sie insbesondere in den europäischen Gremien verfolgt wird, im Wesentlichen unterstützt.

Schrems vermittelt nicht nur der NormalverbraucherIn den Datenschutz in allgemeinverständlicher und unterhaltsamer Art, sondern liefert damit zugleich in knapper aber umfassender Weise eine Gesamtdarstellung der Lage des modernen Datenschutzes und seiner Perspektiven. Mit seiner saloppen Sprache erfreut er LeserInnen, die mit Ironie und Ernsthaftigkeit zugleich umgehen können. Schade ist, dass die Rechtschreibung immer wieder zu Wünschen übrig lässt. Das Buch ist allen zu empfehlen, die sich – egal aus welcher Motivation – für den Datenschutz inter-

essieren: EinsteigerInnen wie SpezialistInnen, Mitarbeitende der Datenschutzbürokratie, VertreterInnen von IT-Unternehmen, vor allem auch PolitikerInnen. Hier erläutert ein junger Nerd, wie uns eine IT-Industrie zulasten eines für die demokratische Informationsgesellschaft zentralen Grundrechtes wegen ihrer kommerziellen Interessen an der Nase herumführt, und wie wir uns wehren können. Er gibt Tipps – eher für andere Nerds – zum technischen Selbstdatenschutz und wie VerbraucherInnen und BürgerInnen ihre gesetzlichen Betroffenenrechte einfordern können.



Von dem Bussche, Axel Frhr./Voigt, Paul
Konzerndatenschutz
Rechtshandbuch
C.H.Beck München 2014,
ISBN 978-3-406-66113-6, 415 S.

(TW) Das Rechtshandbuch, verfasst von PraktikerInnen aus dem Bereich des internationalen Unternehmensdatenschutzes (von dem Bussche, Egle, Hullen, Kamp, Moos, Oenning, Plath, Spies, Voigt, Wedde), behandelt spezielle Fragen, wie sie insbesondere in großen und mittleren (internationalen) Konzernen auftreten. Es zielt auf Rechtsabteilungen, UnternehmensberaterInnen, RechtsanwältInnen, interne und externe Datenschutzbeauftragte sowie Mitarbeitende von Datenschutzaufsichtsbehörden. Bearbeitet sind zentrale allgemeine Themen der personenbezogenen Datenverarbeitung im Unternehmen (Datenschutzmangement, Auftragsdatenverarbeitung, Beschäftigtendatenschutz) wie auch spezielle Themen wie z. B. konzerninterne Übermittlung, internationaler Datenverkehr (incl. Standardvertragsklauseln, Safe Harbor, Binding Corporate Rules), Compliance, Unternehmensverkauf (M&A, Mergers&Acquisitions), E-Discovery und Cloud Computing.

Das Buch erhebt nicht den Anspruch eines umfassenden Handbuchs für den Unternehmensdatenschutz und befasst sich deshalb z. B. auch nicht mit Fragen des Internet- bzw. Telemedienrechts oder dem technischen Datenschutz. Die rechtlichen Darstellungen sind umfassend im Überblick und insofern als Einstieg in viele internationale oder konzernbezogene Fragen ideal geeignet. Dabei werden Streitstände und unterschiedliche Positionen dargestellt, was es dem Unternehmensdatenschützenden ermöglicht, Risiken bei bestimmten Verarbeitungen einzuschätzen und zugleich eine optimale – auch interessensgeleitete – Vorgehensweise zu entwickeln. Die Darstellungen sind nicht parteiisch, wohl ist es aber das Ziel aller AutorInnen, den Datenschutz im Konzern zu optimieren. Für eine vertiefte Problemklärung bleibt es dann oft nötig, die umfangreich zitierten Originalquellen (Kommentare, Zeitschriftenbeiträge, Behördenveröffentlichungen) zu Rate zu ziehen. Fazit: Eine sinnvolle Hilfe für alle, die mit Rechtsfragen des internationalen Konzerndatenschutzes zu tun haben.



Simitis, Spiros (Hrsg.)
Bundesdatenschutzgesetz
Nomos Baden-Baden, 8. Aufl. 2014,
ISBN 978-3-8487-0593-1, 2072 S.

(TW) Je mehr das Bundesdatenschutzgesetz ein Auslaufmodell wird, umso mehr Kommentare gibt es hierzu auf dem Buchmarkt. In der jüngeren Zeit sind viele neue Kommentare hinzugekommen, doch diese können nicht wirklich „dem Simitis“ Konkurrenz machen. Dieser kam mit seiner ersten Auflage im Jahr 1992 als Loseblattausgabe auf den Markt. Gegenüber der 7. Auflage ist er erneut um 186 Seiten auf 2072 Seiten zugewachsen. Die Zunahme der Zahl der Kommentare wie auch von deren Seiten ist Ausdruck einer zunehmenden inhaltlichen Differenzierung wie auch der zunehmenden Relevanz des Themas. Dadurch, dass der Kommentar sich in kurzen Schritten immer weiterentwickeln konnte, ist der Simitis definitiv der vollständigste und materialreichste und inhaltlich ergiebigste Kommentar zum BDSG.

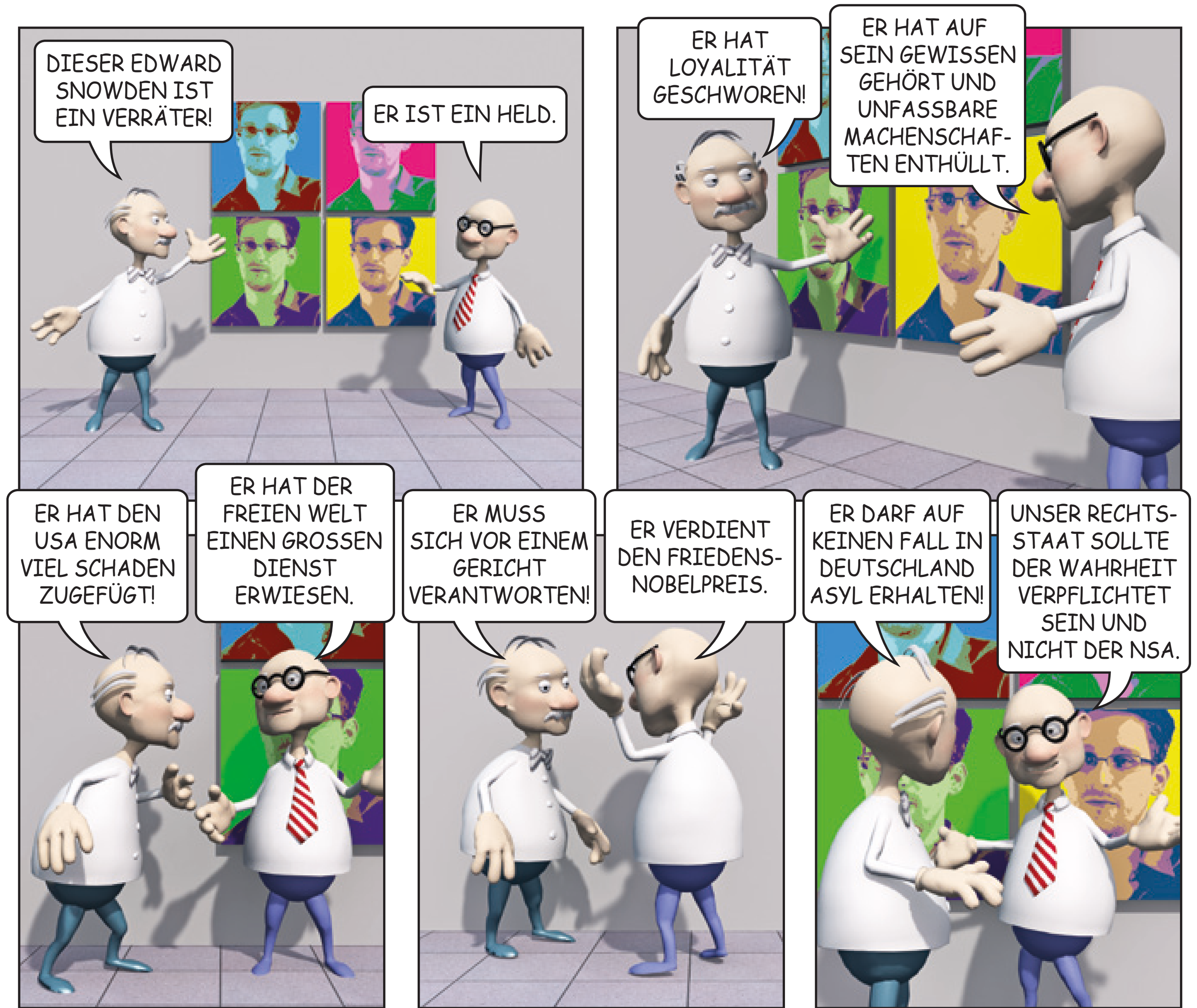
Die meisten rechtlichen Fragen lassen sich alleine mit ihm beantworten. Es bedarf keiner weiteren Literatur. Dies gilt aber nur für die konkrete Anwendung des BDSG. Datenschutzrechtliche Spezialmaterien – auch wenn sie große Überschneidungen mit dem BDSG haben – z. B. das Telemedienrecht oder der Medizindatenschutz mit seinem Patientengeheimnis – werden im Simitis weiterhin nur am Rande bearbeitet und erfordern Spezialliteratur wie die Beantwortung spezialgesetzlicher Fragestellungen, etwa des Sozialgesetzbuches oder sonstiger besonderer Datenschutzregeln. Die historische Darstellung beginnt nicht mit den Ursprüngen des Datenschutzes, sondern mit den Ursprüngen des BDSG. Der technische Datenschutz wird in einem Paragraphen (§ 9) und ohne umfangreiche weitere Nachweise abgehandelt. Hier wäre auch eine Befassung mit der Schutzzielen wünschenswert gewesen, die inzwischen in viele Landesdatenschutzgesetze Eingang gefunden haben. Der Simitis ist also für den juristischen Praktiker wie für den Wissenschaftler unersetzlich. Zugleich sollte man sich dessen bewusst sein, dass er sich auf die Gesetzeskommentierung beschränkt.

Der Anspruch auf weitgehende Vollständigkeit hat einen langen Produktionsvorlauf zur Folge. So wurde die Bearbeitung schon im Dezember 2013 weitgehend abgeschlossen, spätere

wichtige Entscheidungen wurden bis März 2014 nachgepflegt. Nicht mehr berücksichtigt werden konnte als z. B. die EuGH-Entscheidung zur Google-Suche. Neue Themen finden in einen derartigen Praxiskommentar zumeist erst Eingang, wenn hierzu gerichtliche oder sonstige Entscheidungen gefällt wurden oder allgemein anerkannte Publikationen erfolgten, dann aber mit großer Gewissheit. Die Bearbeitung der einzelnen Paragraphen ist individuell sehr unterschiedlich, aber durchgängig auf hohem Niveau und regelmäßig um umfassende Behandlung der relevanten Themen bemüht. Die AutorInnen sind durch die Bank weg langjährig erfahrene, in der Community anerkannte engagierte Datenschützer: Dammann, Dix, Ehmann, Ernestus, Mallmann, Petri, Scholz, Seifert, Simitis und Sokol. Die vertretenen Ansichten sind durchgängig eher datenschutz- als verarbeitungsfreundlich – auch ein nachhaltiges Markenzeichen, wodurch sich der Simitis von mancher Konkurrenz unterscheidet. Dies ändert aber nichts an der Praxisnähe, die mit der Zahl der Auflagen sogar noch zugenommen hat.

In die aktuelle Auflage sind Ausführungen zum Entwurf einer Europäischen Datenschutz-Grundverordnung mit aufgenommen. Deren Verabschiedung und Inkrafttreten dürfte das vorläufige Ende dieser Kommentierungsreihe darstellen. Der Kommentar zielt darauf ab, mit seinen Positionen die Genese dieser Grundverordnung positiv im Sinne des Datenschutzes zu beeinflussen. Zu hoffen ist, dass dann auf der neuen regulativen Grundlage die Grundidee dieses Großkommentars weiterverfolgt wird. Äußerst erfreulich ist die Tradition, die relevante Literatur zu erfassen und die relevanten Gerichtsentscheidungen, von denen es zunehmend viele gibt, in chronologischer Folge zu dokumentieren. Die Handhabbarkeit wird durch eine gute Gliederung, durch ein Abkürzungs- und ein Stichwortverzeichnis erhöht. Es hat sich also nichts geändert: Ernst zu nehmende Datenschutzpraktiker kommen an dem Simitis nicht vorbei.

Cartoon



Ist es nur noch eine Frage der Zeit, bis Anonymität zum Straftatbestand erklärt wird?

